



JUSTIS Information System for the District  
of Columbia

Phase 3 Project file

## **Justice Information System for the District of Columbia**

### **Phase 3 Blueprint**

---

#### **Document History**

Document Filename:	JUSTIS Phase 3 Blueprint v3
Document Type:	Phase 3 Technical Architecture
Document Status:	Final
Time of Last Update:	2/25/2003 7:27 AM
Project Name:	DC JUSTIS Phase 3
Contract Number:	DS-C-0-920-S-065
Document Purpose:	This document details the technical architecture of JUSTIS as of the end of Phase 3 development.
Revision History	9/14/2001 – JUSTIS Phase 2 Final Blueprint 5/7/2002 – JUSTIS Phase 3 Blueprint Draft 12/15/2002 – JUSTIS Phase 3 Review 2/12/2003 – JUSTIS Phase Final ITLO Approval 2/20/2003 – ITAC Review and Approval

~ Table of Contents ~

<b>1. INTRODUCTION</b>	<b>5</b>
1.1 BACKGROUND	5
1.2 IMPLEMENTATION STRATEGY	7
1.3 BLUEPRINT FORMAT	9
<b>2. JUSTIS BUSINESS REQUIREMENTS AND GOALS</b>	<b>12</b>
2.1 JUSTIS BUSINESS REQUIREMENTS	12
2.2 JUSTIS GOALS	13
2.2.1 <i>Collaboration</i>	13
2.2.2 <i>Information Sharing</i>	14
2.2.3 <i>Effective Resource Utilization</i>	14
2.2.4 <i>Information Management</i>	15
<b>3. FUTURE JUSTIS USER COMMUNITY AND SYSTEM</b>	<b>16</b>
3.1 INTRODUCTION	16
3.2 AGENCY INFORMATION SHARING AND COLLABORATION	17
3.2.1 <i>Agency Data Sharing</i>	22
3.3 SUMMARY OF DATA CONTRIBUTION	23
3.4 OTHER INTERAGENCY FUNCTIONS SUPPORTED JUSTIS	24
3.4.1 <i>Notification Services: Publish and Subscribe</i>	25
3.4.2 <i>Collaborative Services: Discussion Groups</i>	26
3.4.3 <i>Data Transfer</i>	28
3.4.4 <i>Data Quality Alliance</i>	29
3.4.5 <i>Public Access</i>	31
3.5 TECHNICAL ARCHITECTURE	35
3.5.1 <i>Full Security Implementation</i>	35
3.5.2 <i>Overall JUSTIS Building Blocks: Web Application Development Standards</i>	36
3.5.3 <i>Physical Plant Design of JUSTIS Components</i>	41
3.5.4 <i>Scalability, Performance Requirements</i>	46
3.5.5 <i>User Workstations</i>	47
3.5.6 <i>Network Infrastructure: Special Security Considerations</i>	48
3.5.7 <i>Application Development Guidelines</i>	48
3.5.8 <i>Off-line, Replicated, Screen-scraped and On-line Data</i>	48
3.6 MANAGEMENT AND ADMINISTRATIVE STRUCTURE	51
3.6.1 <i>JUSTIS Organization Chart</i>	51
<b>4. CURRENT SYSTEMS SUMMARY</b>	<b>61</b>
4.1 SECURITY INFRASTRUCTURE	62
4.2 NETWORK INFRASTRUCTURE	64
4.3 JUSTIS LEGACY SYSTEMS	66
4.4 CURRENT NETWORK DESIGN	68
4.5 USER WORKSTATIONS	70
4.6 JUSTIS POC	71
4.6.1 <i>Proof of Concept Infrastructure</i>	71
4.6.2 <i>POC Operations</i>	72

4.6.3	<i>POC Accomplishments</i>	73
4.7	JUSTIS PHASE 2	73
4.7.1	<i>Phase 2 Infrastructure</i>	74
4.7.2	<i>Phase 2 Operations</i>	75
4.7.3	<i>PHASE 2 Accomplishments</i>	75
4.8	JUSTIS PHASE 3	77
4.8.1	<i>Phase 3 Infrastructure</i>	77
4.8.2	<i>Phase 3 Operations</i>	77
4.8.3	<i>Phase 3 Accomplishments:</i>	78
4.9	SUMMARY	81
<b>5.</b>	<b>ROADMAP</b>	<b>82</b>
5.1	INTRODUCTION	82
5.2	GAP AREAS PRIORITIZED	83
5.2.1	<i>Necessary and Required</i>	85
5.2.2	<i>Realistically Achievable</i>	89
5.2.3	<i>Vision Oriented</i>	91
5.3	PROPOSED PHASES OF IMPLEMENTATION	93
5.3.1	<i>Phase 4 –Second Chance Data Contribution</i>	93
5.3.2	<i>Phase 5 –Expansion of Core Data Transfer</i>	94
5.3.3	<i>Phase 6 –Increased Functionality – Secure Email</i>	95
5.3.4	<i>Phase 7 –Increased Functionality – Systematic Expansion</i>	96
5.3.5	<i>Phase 8 –Vision Oriented</i>	97
<b>6.</b>	<b>CONCLUSION</b>	<b>98</b>
6.1	JUSTIS BLUEPRINT	98
<b>7.</b>	<b>GLOSSARY</b>	<b>99</b>

**~ Figures ~**

Figure 1 – Representative of JUSTIS Phased Implementation.....	8
Figure 2 – Blueprint Format .....	10
Figure 3 – Blueprint Building Metaphor .....	16
Figure 4 – JUSTIS Information Sharing Modes .....	19
Figure 5 – JUSTIS Inquiry Application Flow.....	20
Figure 6 - JUSTIS Interagency Access Chart .....	23
Figure 7– Screen Capture of a Discussion Group .....	28
Figure 8 - JUSTIS DQA Business Process .....	30
Figure 9 - CJCC "I Want To Know..." Homepage.....	32
Figure 10 - CJCC "I Want To Know..." Offender Data.....	33
Figure 11 - CJCC "Yo Quiero Saber..." Homepage .....	34
Figure 12– Three Tier Architecture .....	40
Figure 13– Communication between User Interface and Business Logic Tiers.....	40
Figure 14– Communication between Business Logic and Backend Database Tiers .....	41
Figure 15– JUSTIS Hub and Spoke Structure .....	42
Figure 16– JUSTIS Hub Components.....	45
Figure 17– Areas to Examine for Performance Improvements .....	46
Figure 18– Direct Access .....	49
Figure 19– Replicated Access .....	49
Figure 20– Off-line Access.....	49
Figure 21– JUSTIS Organization Chart .....	52
Figure 22 – Justice Agency Connection Points.....	64

Figure 23 – JUSTIS Phase 3 Technical Architecture .....	69
Figure 24 - JUSTIS Phase 3 Database Diagram .....	70
Figure 25 – JUSTIS POC Network Diagram .....	72
Figure 26 - JUSTIS Phase 2 Architecture .....	75
Figure 27 – Blueprint Format .....	83
Figure 28 - JUSTIS Priority Matrix.....	85
Figure 29 – Current JUSTIS Administrative and Management Structure.....	86
Figure 30 – Future JUSTIS Administrative and Management Structure .....	87

# 1. Introduction

## 1.1 Background

The Criminal Justice Coordinating Council of the District of Columbia (CJCC) was organized with the following mission:

To serve as the forum for identifying issues and their solutions, proposing actions, and facilitating cooperation that will improve public safety and the related criminal and juvenile justice services for District of Columbia residents, visitors, victims, and offenders. The CJCC draws upon local and federal agencies and individuals to develop recommendations and strategies for accomplishing this mission. Our guiding principles are creative collaboration, community involvement, and effective resource utilization. We are committed to developing targeted funding strategies and comprehensive management information through integrated information technology systems and social science research in order to achieve our goal.<sup>1</sup>

In 1999, the CJCC of the District of Columbia, supported by its Policy and Budget Working Group (P&BWG), produced a federal funding strategy, recommended a governance structure, and prepared an *Information Technology Interagency Agreement* that the CJCC members adopted. This agreement recognized the need for immediate improvement of information technology in the criminal justice system within the District of Columbia and established the Information Technology Advisory Committee (ITAC) to serve as the governance body for justice system development.

The ITAC has been given the duty of advising and making recommendations to the CJCC in regards to improvement of the information technology infrastructure of justice agencies within the District of Columbia. The recommendations are to be made in respect to increased funding of information technology projects; increased data sharing, access, and integration; improved data and system security, and the development of system-wide standards and measurement of data use and quality, as appropriate to the then-current developmental stage of the justice system. The recommendations by the ITAC are developed based on the following guiding principles:<sup>2</sup>

Recognize the primacy of each justice agency mission

---

<sup>1</sup> <http://www.cjccdc.dc.gov>

<sup>2</sup> *Ibid.*

Facilitate collaborative solutions to justice information challenges

Commit to the quality and integrity of justice data

Implement effective data and system security

Respect the confidentiality of information and individual privacy

Establishment of system-wide standards, supported by common identifiers and positive identification

Nurture agency and community requirements for research and public access

Provide for long-term performance monitoring and evaluation

Early during the formation of the ITAC, the CJCC recognized that the information systems maintained by the justice agencies within the District were difficult, if not impossible to access. The ITAC envisioned a system that would promote the sharing of justice data while maintaining the primacy of each justice agency. The solution is a District of Columbia Justice Information System (JUSTIS).

In July 2000, the CJCC partnered with the Office of the Chief Technology Officer (OCTO) in contracting BearingPoint, Inc. to design a solution concept that is based on modern dedicated Intranet and web browser technologies that support secure, confidential data access, data sharing, and notification functionality. It is imperative that the solution concept is designed without any disruption of the existing legacy systems of the individual agencies or demand costly and inefficient data collection and transfer. The design was delivered to the ITAC in the form of a JUSTIS Blueprint. In conjunction with the delivery of the JUSTIS Blueprint, BearingPoint, Inc. was also contracted to develop a functioning proof-of-concept (POC). This POC became the initial phase of JUSTIS development and was to serve as a model of data sharing functionality between several CJCC member agencies. Both the JUSTIS Blueprint and the POC were delivered to the ITAC on January 17, 2001.

As a result of the successful demonstration of a data sharing functionality between CJCC member agencies, the CJCC decided to continue the development and implementation of JUSTIS. The CJCC partnered with OCTO to contract with BearingPoint to develop and implement additional data sharing capabilities among member agencies. This extended the development of JUSTIS under the project title, JUSTIS Phase 2. The expansion of JUSTIS during the second phase of development was completed and delivered on September 30, 2001.

In April of 2002, the CJCC again partnered with BearingPoint in order to increase the functionality of JUSTIS. In addition to increasing the functionality of JUSTIS, BearingPoint was contracted to maintain system operations, support and manage

the help desk. This development of increased functionality was titled JUSTIS Phase 3, which lasted from April 2002 through September 2002.

Increasing agency collaboration was the underlying objective of these new functionalities. This increase in agency collaboration was pursued with BearingPoint in the form of three tasks, Core Data Transfer, Data Quality Alliance, and Public Access. These three functionalities not only increase agency collaboration, but integrate JUSTIS into the business processes of all participating agencies, thus making JUSTIS a business critical application.

## 1.2 Implementation Strategy

This document is the JUSTIS Phase 3 Blueprint for the implementation of JUSTIS and the foundation for the CJCC envisioned solution. The JUSTIS Blueprint is a vision of the ultimate system, an analysis of current state capabilities and requirements, and a definition of steps to take for a multi-phased implementation. This Blueprint also provides a high-level architecture and roadmap for the continued development of JUSTIS.

The JUSTIS Blueprint was developed with the intention of a multi-phased approach. A multi-phased implementation is designed to provide enhanced JUSTIS functionalities within a three- to six-month time frame for each phase. Such an implementation provides several advantages over a large, full-scale implementation. A phased implementation:

- Provides short-term successes

- Allows for validation of the long-term plan after each phase

- Allows for the integration of current technologies throughout the implementation

A representative diagram of a possible JUSTIS multi-phased implementation follows:



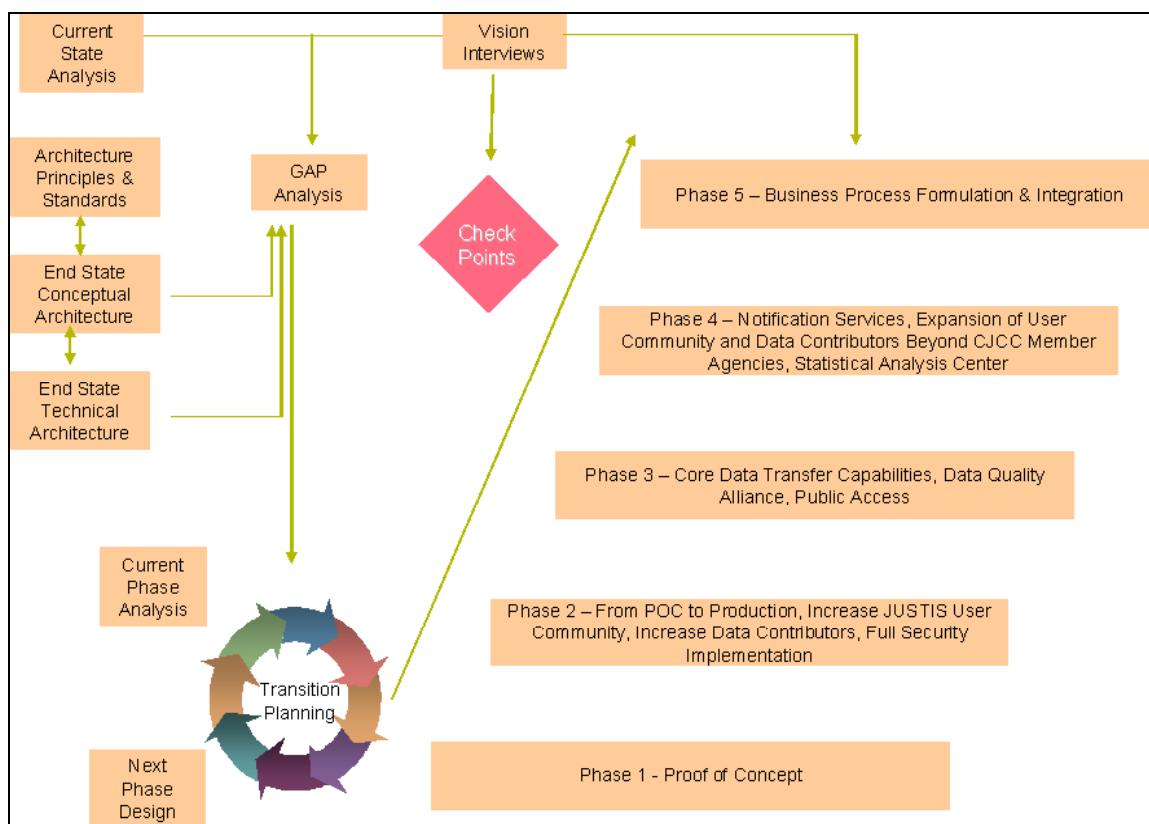


Figure 1 – Representative of JUSTIS Phased Implementation

The beginning of a multi-phase implementation as represented in Figure 1 is an analysis of the current state of the justice agencies' business processes and information technology infrastructure. Coinciding with this analysis is the coordinating of key justice agency personnel's insights in the form of "Vision Interviews." System validation points are developed from the Vision Interviews.

The fully functional JUSTIS system is considered "End State" in the figure. The JUSTIS design is derived from a foundation of agreed upon architecture principles and standards. The JUSTIS architecture is refined by these agreed upon principles and standards. The technical architecture of the system is generated from the conceptual architecture. This evolution of the design of JUSTIS creates the End State solution.

Transition planning is the assessment of the current state analysis and the end state solution that generates a list of "gap" points. The gap points are logically prioritized according to both business and technological constraints and the aforementioned Vision Interviews. The prioritization of the gap points forms the phases in the multi-phased implementation. Throughout the multi-phased implementation each phase

must be validated against the original vision of JUSTIS to ensure the implementation remains true to that vision. However, if a particular area of the vision is proven to be unrealistic or is unable to be followed, then the vision should be updated to reflect reality.

The JUSTIS multi-phased implementation began with the development and deployment of the working proof-of-concept (POC), which was completed in January 2001. The POC used open Internet technologies and standards to link information from diverse justice agency systems as designed in the complete JUSTIS architecture. The POC gave the CJCC and the selected pilot agencies an early look at the JUSTIS architecture and functionality. Also, selected authorized users were granted access to JUSTIS. This enables users to view the selected shared information and observe and actively participate in the on-going development of JUSTIS.

Upon ITAC approval and acceptance of the POC, JUSTIS Phase 2 began. The objective of this phase was primarily focused on the expansion of the data sharing capability demonstrated during the POC. At the conclusion of JUSTIS Phase 2, users of the application were able to access justice information from twelve data sources managed by ten agencies. This phase was approved and accepted by the ITAC in September of 2002.

Phase 3 focused on expanding functionality and establishing JUSTIS as a mission critical element of the participating agencies' business processes. In April of 2002, Phase 3 began when BearingPoint was contracted to develop and implement important new tools. Three distinct functionalities known as Core Data Transfer, Data Quality Alliance, and Public Access combined to add greater depth and utility to JUSTIS. In addition, the District of Columbia's Department of Motor Vehicles (DMV) and the juvenile data from the District of Columbia Superior Court (DCSC) were integrated into JUSTIS as data contributors. The successful implementation of these new tools and the integration of the DMV and the DCSC juvenile data were completed in September 2002.

### 1.3 Blueprint Format

The Blueprint defines and recommends the necessary elements for the CJCC to continue the implementation of JUSTIS. The Blueprint accomplishes this in the following manner:

1. **Defining the Future JUSTIS User Community and System.** It is important to define the ideal future system first, without concern for the current capabilities. This ensures maximum creativity on the part of the participants. The ITLO provided BearingPoint with the opportunity for numerous vision interviews with key ITAC members during the months of July and August 2000. The BearingPoint Team also considered capabilities in the BearingPoint JNET

- solution developed for the Commonwealth of Pennsylvania. Details on the future JUSTIS user community and system can be found in section 3.
2. **Defining the current technical infrastructure of the participating justice agencies in the District of Columbia.** The first step defined where we want to end up with JUSTIS. This step describes the point from which we will begin. Details on current technical infrastructure can be found in section 4.
  3. **Conducting a Gap Analysis.** In this step, we show the distance that needs to be closed in moving from the current state towards the target end state. Results of the gap analysis are described in section 5.
  4. **Recommendation of the Roadmap that will bring the Future JUSTIS System to reality in the justice agencies within the District of Columbia.** The roadmap recognizes the importance of a phased implementation, as discussed above. References to the proposed solution for the future of JUSTIS can be found in section 5.

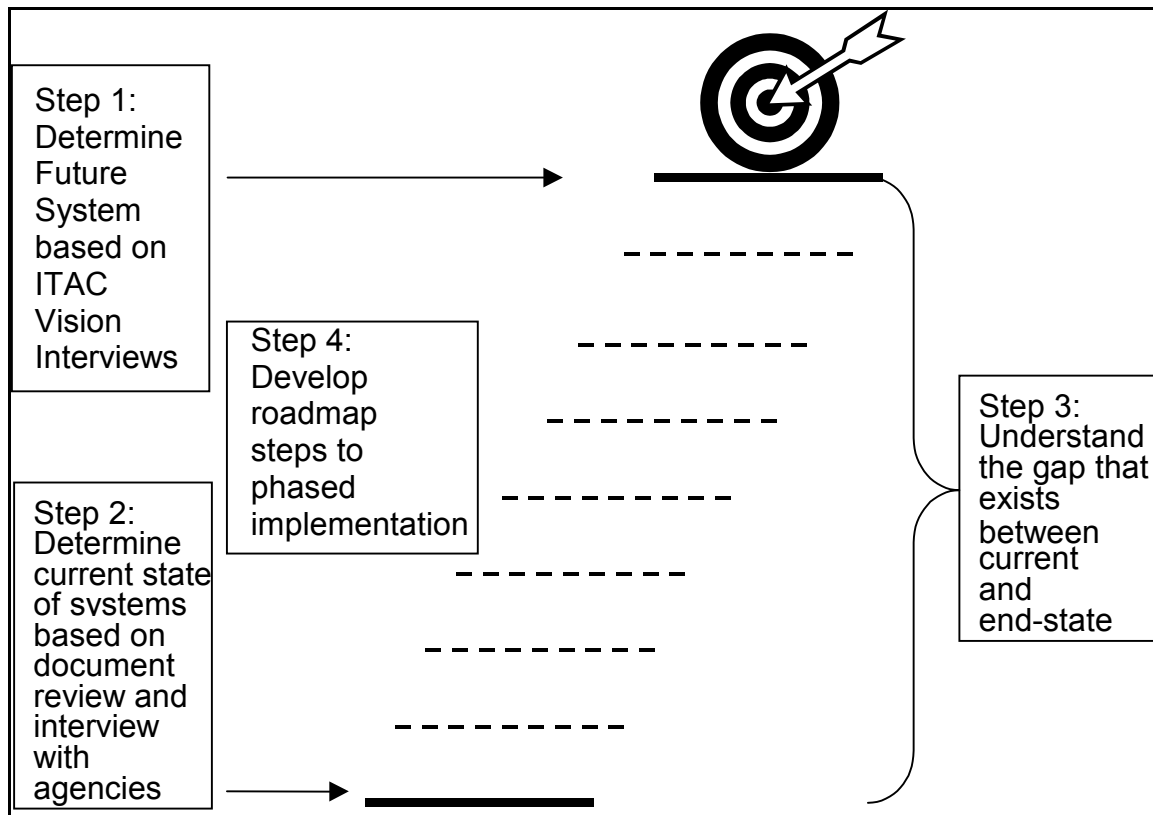


Figure 2 – Blueprint Format

The Blueprint is a “living” document. Therefore, as JUSTIS Phases are developed and implementation paths are followed, it is expected that the Blueprint will be updated in consideration of the following:

- **Initial Phase Definition** – This point is shortly after a Statement of Work (SOW) defined the initial phase. The Blueprint should be updated to include information more specific to the phase as defined in the SOW. The essence of this update is the inclusion of proposed methodologies that will contribute to the success of the phase. This update should also reflect any significant findings gained since the last update.
- **Phase Results** – At this point the implementation team has developed and implemented the functionalities defined by the SOW. The Blueprint is updated to reflect any “lessons learned” during implementation the predefined phase.
- **User Evaluation** – An evaluation period is planned at the end of each phase. At this time the users will be able to express ideas and suggestions about JUSTIS system development. The JUSTIS Blueprint is then updated to include the evaluations and proposed suggestions encompassed in the evaluations.

## 2. JUSTIS Business Requirements and Goals

### 2.1 JUSTIS Business Requirements

The CJCC has taken the initiative in pursuing and managing necessary business requirements within the justice community of the District of Columbia that lead to the accomplishment of its stated objectives. These business requirements are continually referenced throughout the development of JUSTIS.

**Implement industry best practices for information security.** JUSTIS requires system-wide security policies. The CJCC has taken the initiative to develop security policies that meet or exceed the security requirements of the member agencies and draws upon elements from the National Crime Information Center (NCIC) standards.

**Encourage the use of a common District-wide identifier.** The data shared in JUSTIS has been designed to be retrievable by a common District-wide tracking number, based on the Arrest Number. Having a common tracking number will enable many of the functions of JUSTIS and will assist justice agencies within the District in coordinating their information processing. The implementation of a common District-wide tracking number would encourage the development of other functionality that could use this tracking number to link relevant information to the unique criminal justice process and combined with the use of meta data could enable the implementation of statistical analyses without the use of a data warehouse.

**Foster interagency participation and collaboration.** JUSTIS enables participation of all District and Federal justice agencies. JUSTIS ease of use creates an environment that promotes interagency participation and collaboration. Ease of use combined with its leverage of Internet technology allows for public safety interagency participation and collaboration beyond the core CJCC agencies to other law enforcement agencies serving the District of Columbia jurisdiction. This approach avoids any need for re-engineering existing production systems.

**Streamline processing that cross agency boundaries.** The streamlining of agency processes increases efficiency and effectiveness. The implementation of JUSTIS integrates technology into currently manual process. The reduction of manual processes will streamline processes across agency boundaries and improve the integrity of the data being shared.

**Recognize the independence and primacy of each justice agency.** Although agency coordination and consensus is a necessary business requirement, effective agency governance and representation is just as critical. The development of JUSTIS recognizes agency primacy and is designed to be considerate of individual agency decision-making and systems development.

**Employ open technologies.** The use of open technologies also contributes to the independence of individual agencies. Agencies can make changes to other information systems with minimum impact on JUSTIS. Open technologies greatly reduce the effort on the part of new agencies to participate in JUSTIS.

The CJCC is committed to making the many justice agencies within the District of Columbia function in unison with information sharing as a backbone. The District of Columbia's JUSTIS system is designed to provide a platform for this information sharing through the use of "connections." JUSTIS provides connections between people and information (information inquiry applications and search engines); connections between people and people (newsgroups, discussion groups, secure email) and connections between information and information (e.g., data transfer, data quality, notification). JUSTIS is designed to contribute to the objectives of the CJCC.

## 2.2 JUSTIS Goals

In addition to the business requirements imposed on JUSTIS, there are a number of fundamental goals for the system: collaboration, information sharing, effective resource utilization and information management.

### 2.2.1 *Collaboration*

JUSTIS offers a central secure portal that fosters the development of the District's criminal justice community while providing a platform for the collaborative solutions to justice information challenges. JUSTIS increases the ability of agencies to work together in case management and transmission of data. A basic example is the publication of an offender contact list that is made available through JUSTIS. This offender contact list will provide the contact information for case handlers, such as the attorneys assigned to the case, the judge assigned, the arresting law enforcement official, and any other individuals within the justice agencies that could be of importance. The list would provide one area to obtain key contacts for an individual offender.

Notification Services is to be incorporated in JUSTIS in order to provide yet another opportunity for justice agency collaboration. Notifications can be delivered on an individual basis, agency basis and/or a group basis. For example, when a parolee is arrested and booked, this event (the police booking) can generate a notification to an individual parole officer, group of interested parties or the entire offender supervision agency.

Another opportunity for collaboration is through the use of discussion groups. Authorized users could participate in on-line discussions regarding justice issues, case management, or the sharing of critical investigative information.

Secure email offers yet another opportunity for collaboration that is to be implemented. Secure email provides criminal justice officials confidence in communications. Justice officials can communicate with other officials within the justice community and be confident in the other official's identity.

### 2.2.2 *Information Sharing*

Interagency sharing of data supports each agency's ability to make quality decisions. JUSTIS provides a platform for the sharing of critical justice information on a timely basis and in a secure environment. This allows justice agencies to share selected information that will assist each justice agency in conducting its mission-critical activities.

The CJCC decision to take advantage of modern dedicated Intranet and web browser technologies allows for the publishing of data in a timely fashion. One example of an information sharing opportunity that can be enhanced with the implementation of JUSTIS is the accurate identification of court appointed attorneys. Any change in attorney assignment made by the courts can be "published" (translated to a standard web-accessible format and forwarded) using JUSTIS. Any authorized JUSTIS user could then locate and retrieve the current case disposition of an offender.

Information sharing is further enhanced through the implementation of data transfer functionality. This is the natural progression to information sharing through publication. Through this functionality, data sharing increases in value as critical data is directly loaded into agency information systems in a timely fashion. This eliminates a number of manual data entry processes present throughout the justice community today. An example of the data transfer functionality made available through the implementation of JUSTIS, is the transfer of MPDC arrest data to all authorized CJCC agencies. Given the overwhelming need for arrest data throughout the justice agencies, data transfer functionality provides this data more timely and accurate than through any other process used before. It also reduces data entry errors that can occur when agencies are forced to re-key data from one information system into another.

### 2.2.3 *Effective Resource Utilization*

Before JUSTIS, interagency data exchanges were often either not taking place or are performed using inefficient manual processes. JUSTIS allows agencies to

use information system solutions to become more effective contributors and reduce labor-intensive information searches. For example, many justice agencies are in need of the daily “arrest list” produced by the Metropolitan Police Department of the District of Columbia (MPDC). Formerly, the acquisition of this list in a timely manner by each agency requires labor-intensive processes. The implementation of JUSTIS has allowed the arrest list to be published in a relatively short time frame from when it is produced by MPDC, therefore eliminating any need for other agencies to commit resources in the acquiring of this list.

Alternatively, JUSTIS allows for the arrest list to be made available through download functionality via the data transfer functionality. The concept allows for common data to be identified and captured through the browser. The authorized user could then potentially copy the data and use it to populate a corresponding common data field in the agency’s legacy system. This again, eliminates the redundant activity of re-keying common information from system to system. Therefore reducing potential errors caused by keying mistakes when transferring data from system to system.

#### *2.2.4 Information Management*

Information systems for the justice community must implement effective data and system security. JUSTIS provides for indirect data retrieval from agency information systems. This allows for a significant decrease in security risk to the legacy systems and absolutely no risk of data corruption. Authorized users enter JUSTIS and view published data that has been obtained either through direct access through a firewall to the legacy system, indirect access through a firewall to an intermediary server, or off-line access, where the data is loaded into the JUSTIS agency server through some other media. Thus the inquiry does not have constant direct unsecured access to the agency legacy system.

Additionally, a tenet of JUSTIS is to not interfere with, compete with, or replace current legacy systems. **JUSTIS is not a data warehouse.** Therefore there is no central repository of data and the data physically stays within the agency’s IT infrastructure unless otherwise requested by the particular agency. JUSTIS allows for data sharing of critical information without the enormous effort to standardize data elements across many autonomous agencies.



### 3. Future JUSTIS User Community and System

#### 3.1 Introduction

JUSTIS supports the justice community and each of its member agencies. This section describes the fully functional system, the model that comprises the overall solution, the proposed user community, the technical architecture, and the organizational structure necessary to manage and administer the system.

This section concentrates on describing the future “to be” JUSTIS system. Subsequent sections will address the current state and strategies for getting from where we are to where we want to be. Because this is a Blueprint document, it seems appropriate to use the following building metaphor to organize this section:

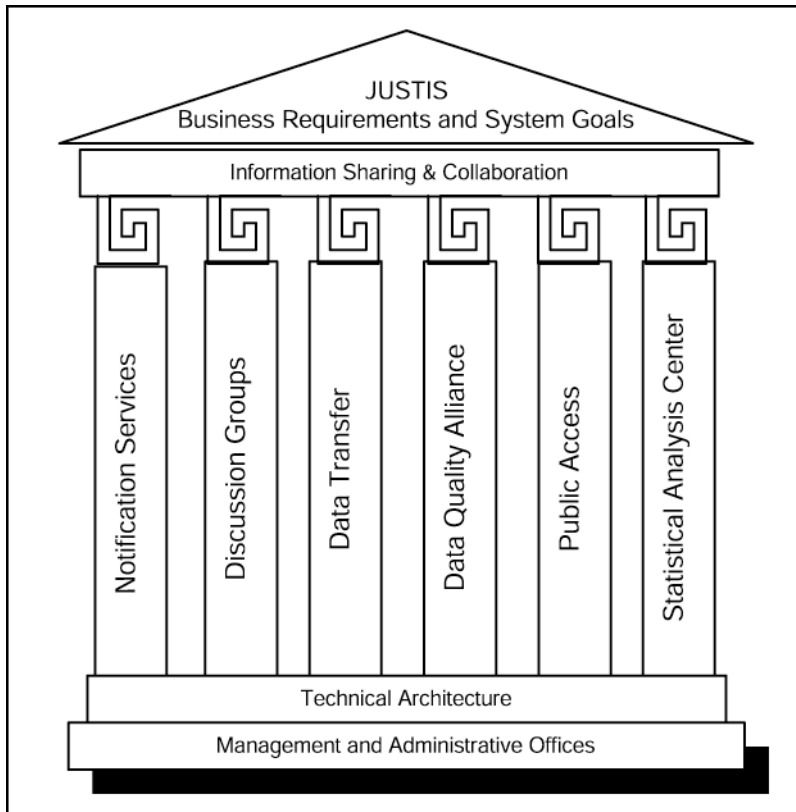


Figure 3 – Blueprint Building Metaphor

In this section, we will explain each structural aspect of the building by starting from the top of the diagram and proceed toward the bottom. This provides for a sense of

dismantling the structure from its outermost components in order to explain its supporting parts.

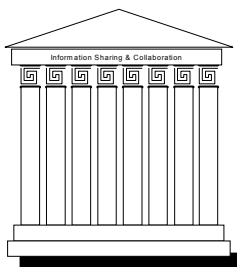
We have already discussed the business requirements and system goals that JUSTIS is designed to meet. In this section, we will discuss the functional components that empower JUSTIS and its users to achieve the business requirements and system goals. “Information Sharing and Collaboration” is shown across the top of our diagram because it is the very essence – the capstone – of the system. (See section 3.2 Agency Information Sharing )

We will present the supporting functional components. Shown as columns in the diagram, these functions of JUSTIS support information sharing and collaboration. (See section 3.4 Other Interagency Functions Supported JUSTIS)

Later, we will present the technical architecture that is needed to support the functional components. The functional discussion has shown *what* the system will do. The technical architecture section will show *how* the system will do it. (See section 3.5 Technical Architecture)

Finally, the management and administrative office structure necessary to support JUSTIS is described. Shown at the bottom of our diagram, this organization will be the bedrock and foundation for JUSTIS. (See section 3.6 Management and Administrative Structure)

## 3.2 Agency Information Sharing and Collaboration



JUSTIS is designed to provide justice agencies a quick and effective way to share justice information and collaborate with colleagues. The value provided by JUSTIS to the user community is in direct relation to the number of participating agencies – both contributors and consumers.

JUSTIS enables its users to share justice information through a variety of modes:

**JUSTIS Data Inquiry Applications** – Queries allow individual JUSTIS agencies to view the public safety data located in other agencies’ information systems. Whether it be adult criminal data searches, juvenile data searches or simply DMV information requests, authorized users access the inquiry application, enter queries based upon agency system keys or the District of Columbia Public Safety Tracking Number (As defined in District of Columbia Public Safety Design Document), fills the query requirements and submits. The system returns a unified view of queried information.

This inquiry can be done across all contributing agencies or by individual agency. Note that queries, logins and other user activity are recorded to an audit log.

**Searches** – Information sharing is improved beyond predetermined queries when information searches are enabled. These searches can be conducted across the entire World Wide Web or within the JUSTIS framework of static pages and other content.

**Static Screens and Printed Reports** – Agencies are able to share information through the publishing of static screens. Static screens display content in Hypertext Markup Language (HTML) and are delivered to a web browser using Hypertext Transfer Protocol (HTTP). This information is not dynamic; therefore it cannot be changed due to user input. The ability to publish agency reports on the web is an efficient form of information dissemination. Agency reports can be published in HTML as well as PDF formats using the appropriate “plug-in” software. Authorized users can download these published reports.

**Data Transfer** – Data transfer is the pinnacle of information sharing and a natural extension to the data inquiry functionality and notification services. Data Transfer functionality consists of redundant data being either pushed or pulled from the data originating agencies to other subscribing agencies. This reduces human intervention involved with the entry of data into agency systems, hence reducing the probability for errors that can promulgate and lead to reduced data quality.

The strategy used in designing the data transfer functionality is dependent upon the agency data access methodology. Data access directly into an agency’s operational system invites the use of a messaging middleware. While, the use of data transformation via a common intermediary relational database platform allows the leveraging of Structured Query Language (SQL) stored procedures.

**Notification Services** – Notification services enable data to interact proactively with authorized users. Specifically developed data “triggers” are implemented to analyze data for changes in selected events. This generates a notification to an authorized subscriber. This level of information sharing goes beyond those previously discussed and introduces interactive data.

**Threaded Discussion Groups** – Discussion groups further enhance information sharing by allowing inter-agency interaction. Discussion groups allow authorized users to post messages for response by other authorized users or data administrators.

**Statistical Analysis** – Statistical analysis seeks to provide in depth meaning to the data made available through JUSTIS. Data is combined and analyzed in order to provide the entire community useful information that can be used in agency strategic planning.

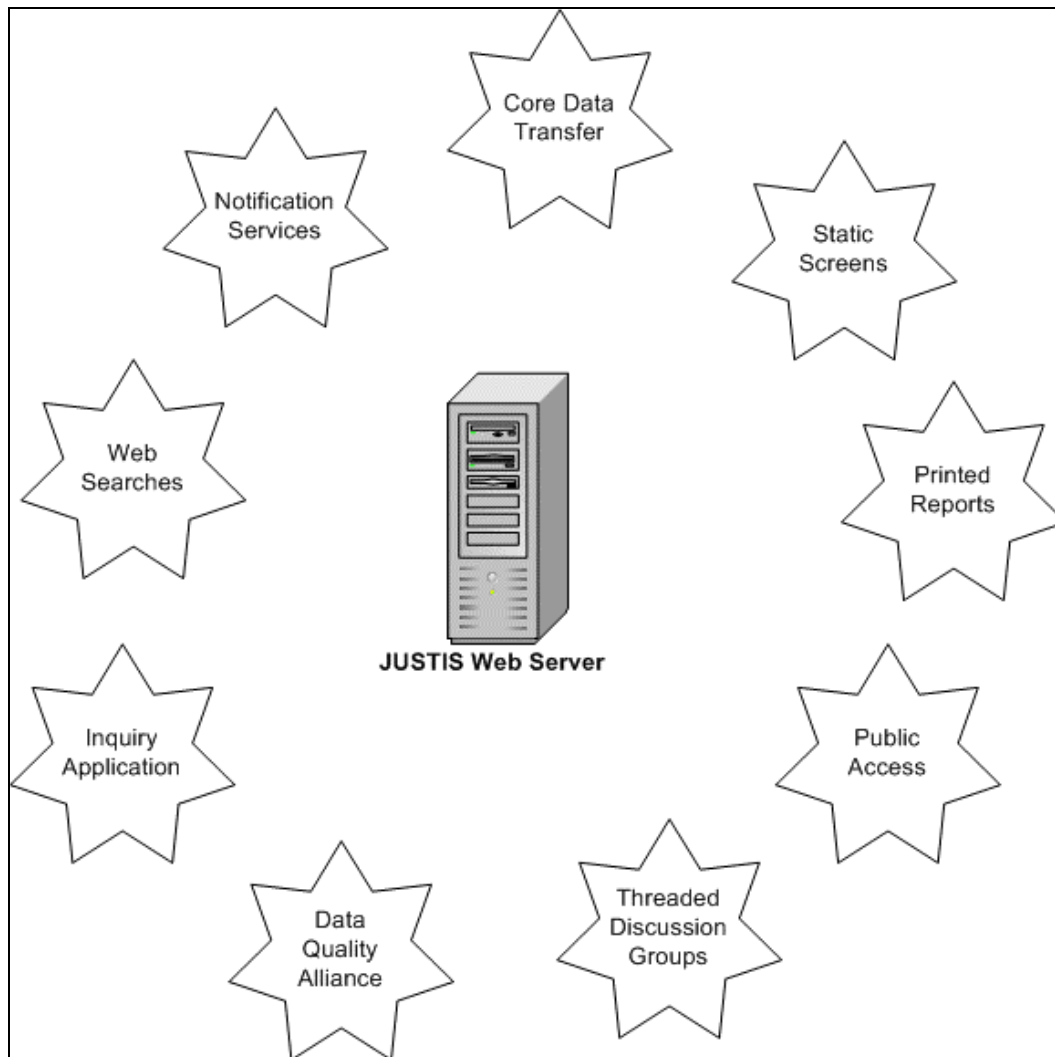


Figure 4 – JUSTIS Information Sharing Modes

Information sharing will be made possible through the use of a secure justice system-wide Intranet. Through JUSTIS, community agencies have a unified view of justice information. Formerly this unified view was not possible because each agency's legacy system holds an individual island of information. JUSTIS connects these islands into a unified system available to answer user queries. This section details the data each agency has chosen to share.

Subsequent sections will provide details on the modes of searches, static screens and printed reports, threaded discussion groups, secure email, data transfer and

notification services. The remainder of this section focuses primarily on the core functionality JUSTIS provides, the JUSTIS Inquiry Application.

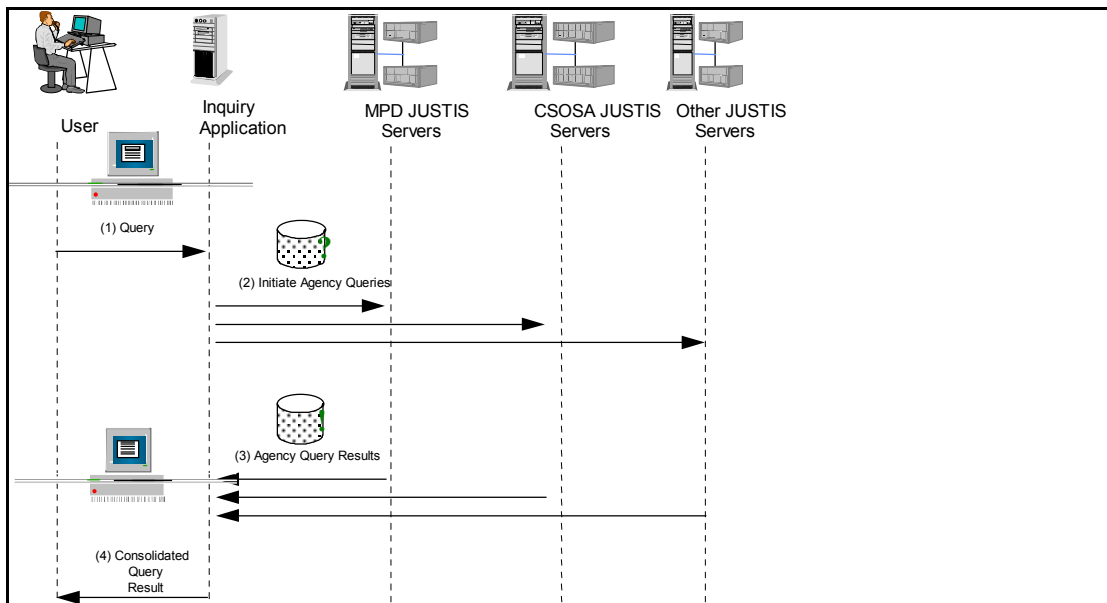


Figure 5 – JUSTIS Inquiry Application Flow

The JUSTIS Inquiry Application provides a justice worker with data from justice agency sources via a single-point search application and user interface. Typically, the data sources will reside in databases controlled by individual agencies.

Search results are organized in a file and folder metaphor. The architecture of this application allows for the ability to incorporate new types (documents) and new sources (agencies) of information as they come on line, without having to rewrite the application or requiring extensive re-configuration. It also restricts access to information found by the search (at least on a document level, if not on a field level).

Individual agencies determine information to be shared and decide upon mechanisms for which JUSTIS will acquire the shared data. Information detailing each agency's selected data contribution methodology is documented in JUSTIS Phase 3 deliverable 1.6, JUSTIS Data Contribution Design Document. This document lists a description of the data each contributing agency has agreed to share through JUSTIS. The Blueprint also provides an illustration of the technical design of the agency data contribution and concludes with the entailing process involved with the agency data contribution.

The JUSTIS contributing agencies that are included in deliverable 1.6 are as follows:

Court Services and Offender Supervision Agency (CSOSA)

District of Columbia Department of Corrections (DOC)

District of Columbia Superior Court (DCSC)

Metropolitan Police Department (MPDC)

Office of Corporation Counsel (OCC)

Pretrial Services Agency (PSA)

United States Attorney's Office (USAO)

United States Parole Commission (USPC)

Youth Services Administration (YSA)

District of Columbia Department of Motor Vehicles (DMV)

As a result of the successful implementation of JUSTIS, agencies outside of the CJCC and the District of Columbia have requested access and the ability to contribute data. This will build upon the original agency expansion accomplished in Phase 2. Currently the United States Probation Office (USPO) and the District of Columbia Child and Family Services Agency (CFSA) have become contributors and are the first of the "next wave" of future JUSTIS participants.

### 3.2.1 *Agency Data Sharing*

Agencies that contribute data determine the access rights to that data. This is usually done on an agency basis. For example, contributing agency A may decide to allow access to their data for agencies B and D but not C. Agency A is thereby delegating to agencies B and D the responsibility to determine which individuals will be approved for JUSTIS access.

A more restrictive level of access can be granted to specific individuals at the discretion of the contributing agency. In this case, the contributing agency will approve the individual application for access. This approach is in place to provide for additional security over highly sensitive data such as information pertaining to juveniles.

The CJCC member agencies have coordinated with the ITLO and the Information Security Officer (ITSO) in developing an Agency Data Access Matrix. This matrix summarizes the data accessibility of user agencies as defined by the contributing agencies. This matrix is the primary basis on which group access is granted.

PENDING

Interagency Contribution / Access Chart

Last Update:

1/27/03

Providing Agencies

Does the agency below allow access by the agency on the left hand column?

Agencies requesting access to JUSTIS data

	BOP	CSFA	CSOSA	DCDC	DCSC	DCSC-J	DMV	MPD	MPD-J	OCC	PDS	PSA	USAO	USPC	USPO	YSA
Federal Bureau of Prisons	NO	NO	YES	YES	YES	NO	YES	YES	NO	YES	YES	YES	YES	YES	NO	NO
Child and Family Services Agency	N/A <sub>a</sub>	NO	NO	YES	YES	YES*	YES	NO	NO	YES	NO	NO	YES	NO	NO	NO
Court Services and Offender Supervision	N/A <sub>a</sub>	NO	NO	YES	YES	NO	YES	YES	NO	YES	YES	YES	YES	YES	NO	NO
D.C. Department of Corrections	N/A <sub>a</sub>	NO	YES	NO	YES	NO	YES	YES	NO	YES	YES	YES	YES	YES	NO	YES
D.C. Superior Court	N/A <sub>a</sub>	NO	YES	YES	NO	NO	YES	YES	NO	YES	YES	YES	YES	YES	NO	YES*
Division of Motor Vehicles	N/A <sub>a</sub>	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO	NO
Metropolitan Police Department	N/A <sub>a</sub>	NO	YES	YES	YES	NO	YES	NO	NO	YES	YES	YES	YES	YES	NO	NO
Office of Corporation Counsel	N/A <sub>a</sub>	NO	NO	YES	YES	YES*	YES	YES	NO	NO	YES	YES	YES	NO	NO	YES*
Public Defender Service	N/A <sub>a</sub>	NO	NO	YES	YES	NO	YES	NO	NO	YES	NO	NO	YES	NO	NO	NO
Pretrial Services Agency	N/A <sub>a</sub>	NO	YES	YES	YES	NO	YES	YES	NO	YES	YES	NO	YES	NO	NO	NO
Office of the United States Attorney	N/A <sub>a</sub>	NO	YES	YES	YES	NO	YES	YES	NO	YES	YES	YES	NO	YES	NO	NO
United States Parole Commission	N/A <sub>a</sub>	NO	YES	YES	YES	NO	YES	YES	NO	YES	YES	YES	YES	NO	NO	NO
United States Probation Officer	N/A <sub>a</sub>	NO	YES	YES	YES	NO	YES	YES	NO	YES	NO	YES	YES	YES	NO	NO
Youth Services Administration	N/A <sub>a</sub>	NO	NO	NO	YES	YES*	YES	YES	NO	YES	YES	YES	YES	NO	NO	NO
Police Coordination Act of 1997 Agencies	NO	NO	SEL	YES	YES	NO	YES	YES	NO	YES	NO	YES	YES	NO	NO	NO

Legend

- YES Access is permitted
- YES\* Access is permitted for selected personnel approved by granting agency
- SEL Access to selected agencies only
- NO Access is NOT permitted
- Time sensitive decision required
- N/A<sub>a</sub> Pending Review of Participation

Figure 6 - JUSTIS Interagency Access Chart

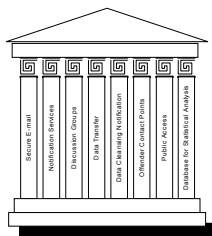
### 3.3 Summary of Data Contribution

The following table summarizes the data that is currently shared through JUSTIS. This table cross-referenced with Figure 6 provides the reader a better understanding of the data that is available through JUSTIS and the agencies that have access to the data.



CJCC Agency	Data Contributed
Metropolitan Police Department	Offender Identification Data Offender Arrest Data Offender Mug Shots
Court Services and Offender Supervision Agency	Probation Supervisory Data
Pretrial Services Agency	Pretrial Data
Public Defender Service	Public Defender Contact Information
D.C. Department of Corrections	Corrections Data
United States Attorney's Office	US Attorney Contact Information
D.C. Superior Court	DC Adult Case Data DC Juvenile Case Data
United States Parole Commission	US Parole Prisoner Data US Parole Decision Documentation
D.C. Office of Corporation Counsel	DC OCC Attorney Contact Information
D.C. Department of Human Services Youth Services Administration	Juvenile Data
D.C. Child and Family Services Agency	Juvenile and Family Data
D.C. Department of Motor Vehicles	DC Driver Information
United States Probation Office Data	Federal Offender Probation Data

### 3.4 Other Interagency Functions Supported JUSTIS



The previous section described the core functionality of information sharing within JUSTIS. This section discusses the individual functions that further enhance the system and empower its users to fully collaborate with one another.

### 3.4.1 Notification Services: Publish and Subscribe

The future JUSTIS system will be designed to allow events within the JUSTIS to trigger notifications to interested and subscribed parties. The notification could be on an individual basis, a group basis or an agency basis. For example, when a parolee is arrested and booked, this event (the police booking) can generate a notification to a parole officer or group of interested parties. The notification can also be generated and sent to one particular point of contact within an agency, to which that point of contact is responsible for distribution of the notification to the interested parties within the agency. This section of the Blueprint will define major events and those who have expressed an interest in notification.

Below is a summary of the possible events and the originating agency that will be triggering the notification.

Event	Source Agency
Adult Arrest	Metropolitan Police Department (MPDC)
Judicial Disposition	District of Columbia Superior Court (DCSC)
Change in USAO Prosecutor	United States Attorney's Office for the District of Columbia (USAO)
Change in DC Prosecutor	Office of Corporation Counsel (OCC)
Change in Defense Counsel	District of Columbia Superior Court (DCSC)
Trial Date Change	District of Columbia Superior Court (DCSC)
Escapes	District of Columbia Department of Corrections (DOC)
Adult Arrest Warrants	Metropolitan Police Department (MPDC)
Adult Bench Warrants	District of Columbia Superior Court (DCSC)
Escape Warrants	District of Columbia Superior Court (DCSC)

Event	Source Agency
Parole Violation Warrants	Court Services and Offender Supervision (CSOSA)
Parole Placements/Releases	United States Parole Commission (USPC)
Walk-away	District of Columbia Department of Corrections (DOC)

During the third phase of JUSTIS a design of a notification system was developed through the use of Joint Application Design (JAD) sessions. The agreed upon JUSTIS Notification System is detailed in JUSTIS Phase 3 Notification Services Design.

Currently, there are three notification related systems currently in existence within the CJCC agencies. Each of these systems is labor intensive and requires manual initiation. Descriptions of all three of these systems are detailed in the JAD session meeting notes. Also included in that document is a list of the required software and hardware to implement a notification system within the District of Columbia.

### *3.4.2 Collaborative Services: Discussion Groups*

JUSTIS provides the environment for threaded discussion groups/forums. A discussion forum is an on-line conference. A JUSTIS system administrator can set up discussion forums, and any other authorized JUSTIS user with a web browser and the proper access can join in and participate in the forums. Unlike Newsgroups, which are open to the public, threaded discussion groups/forums are only available to authorized users. This on-line forum allows users to:

Discuss topics of mutual interest.

Ask questions of anyone in the forum.

Search through message archives by keyword.

Accomplish the data cleansing notification system through a discussion group.

JUSTIS technical help desk questions could be fielded through a discussion group. This would allow both the users and the technical resources to search and review the group's archives for answers to frequently asked questions.

Discussion groups promote a sense of community among members. This capability therefore ties back directly to the JUSTIS business objective of promoting collaboration.

Threaded discussion groups are different from on-line chat. On-line chat takes place in real time, which requires that all participants who want to communicate be logged in and typing at the same time. This makes for a distracting and difficult-to-follow conversation. Threaded discussion groups allow authorized JUSTIS users to view ongoing conversations, post messages to those conversations, and create new conversations at any time convenient to them.

Another difference between on-line chat and threaded discussion groups is that, in on-line chat, once everyone logs off of the chat forum, there may be no record of the conversation. Discussion groups post messages into a discussion database. This allows users to post new messages and view other user's recent and past messages whenever desired. This also allows messages to be indexed and users to search for messages by keyword or other criteria.

Threaded discussion groups are also different from electronic mail. In email, a user's inbox is private to that user. In a discussion group, all members of the group (sometimes referred to as a forum) can see and respond to all messages. The discussion group becomes, in effect, a community in-box.

Discussion groups can be moderated or non-moderated. In a moderated group, a moderator is selected and given special access privileges. When a user posts a message to a moderated group, the message is not made available to the group until the moderator has approved the message for distribution.

The following is an example of the introductory interface of a discussion group:

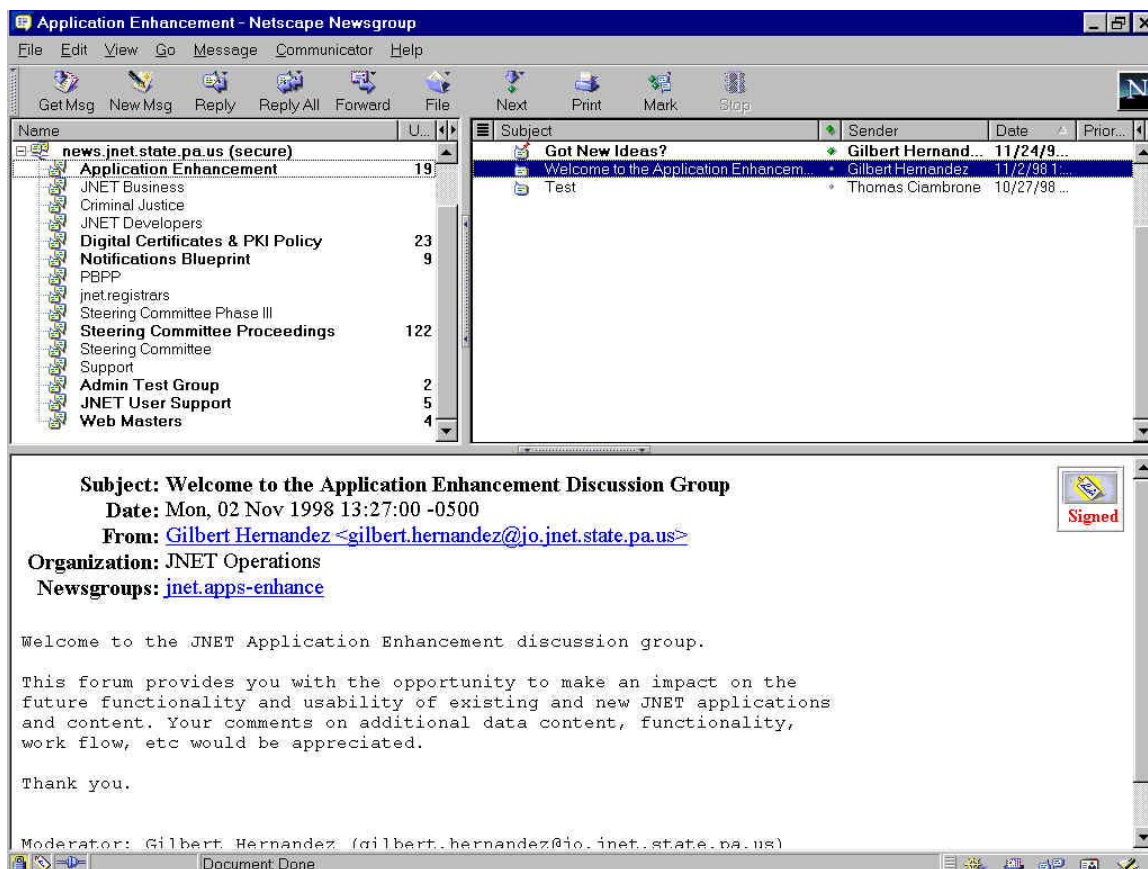


Figure 7– Screen Capture of a Discussion Group

### 3.4.3 Data Transfer

JUSTIS Phase 3 resulted in the implementation of the initial core data transfer functionality. This functionality was designed through the utilization of JAD sessions and developed based upon the agreed design. The details regarding the design and implementation of this functionality are detailed in JUSTIS Phase 3 deliverable number 2.1, JUSTIS Core Data Transfer Design. This document details the data being transferred, the designed process flow, and the agency user interfaces.

Although the initial core data transfer was developed based upon the JAD session resultant design, this functionality and JUSTIS overall can be further enhanced with integration of both the data transfer functionality and the notification services functionality. Both functionalities can be integrated with the implementation of a Message Oriented Middleware (MOM) which would allow for real-time notifications and data transfer.

The initial core data transfer functionality focused on the distribution of arrest data from MPDC to other JUSTIS agencies. The successful implementation of this functionality provides a foundation for further data transfer from other JUSTIS agencies. A natural continuation of the initial arrest data transfer is the implementation of a court core data transfer (CCDT). This functionality would be implemented similarly to the initial core data transfer functionality. With CCDT, the offender data associated with his/her trial will be sent on a very frequent schedule to a JUSTIS supported “push” function. This data will also be temporarily stored in a First-In-First-Out (FIFO) transient database, with file life of 15 days.

### *3.4.4 Data Quality Alliance*

The implementation of a system whereby related information from different sources is viewed requires a business process that provides the mechanism to identify, report, and resolve data inconsistencies. JUSTIS has enabled the District of Columbia criminal justice community to pull together multiple agencies’ views of data, therefore allowing for the first time, the comparison of this data across all contributing agencies. This new capability provided by JUSTIS accommodates a business process whereby the user posts a report via the DQA infrastructure of inconsistencies or suspected errors to another agency’s data quality administrator. The data quality administrator from the agency or agencies is responsible for the coordination and resolution of the data inconsistency. For example, a user retrieves data from MPD that displays an offender’s charge number. This same user notices that the data retrieved from Pretrial Services Agency displays a different charge number. The user could then send an email to either data quality administrator or both requesting the data to be verified and corrected if necessary.

During the third phase of JUSTUS implementation the Data Quality Alliance (DQA) was developed and implemented. This innovative approach to data cleansing, invokes a collaborative multi-agency effort to data cleansing. The graphic below illustrates at a high-level the DQA business process.

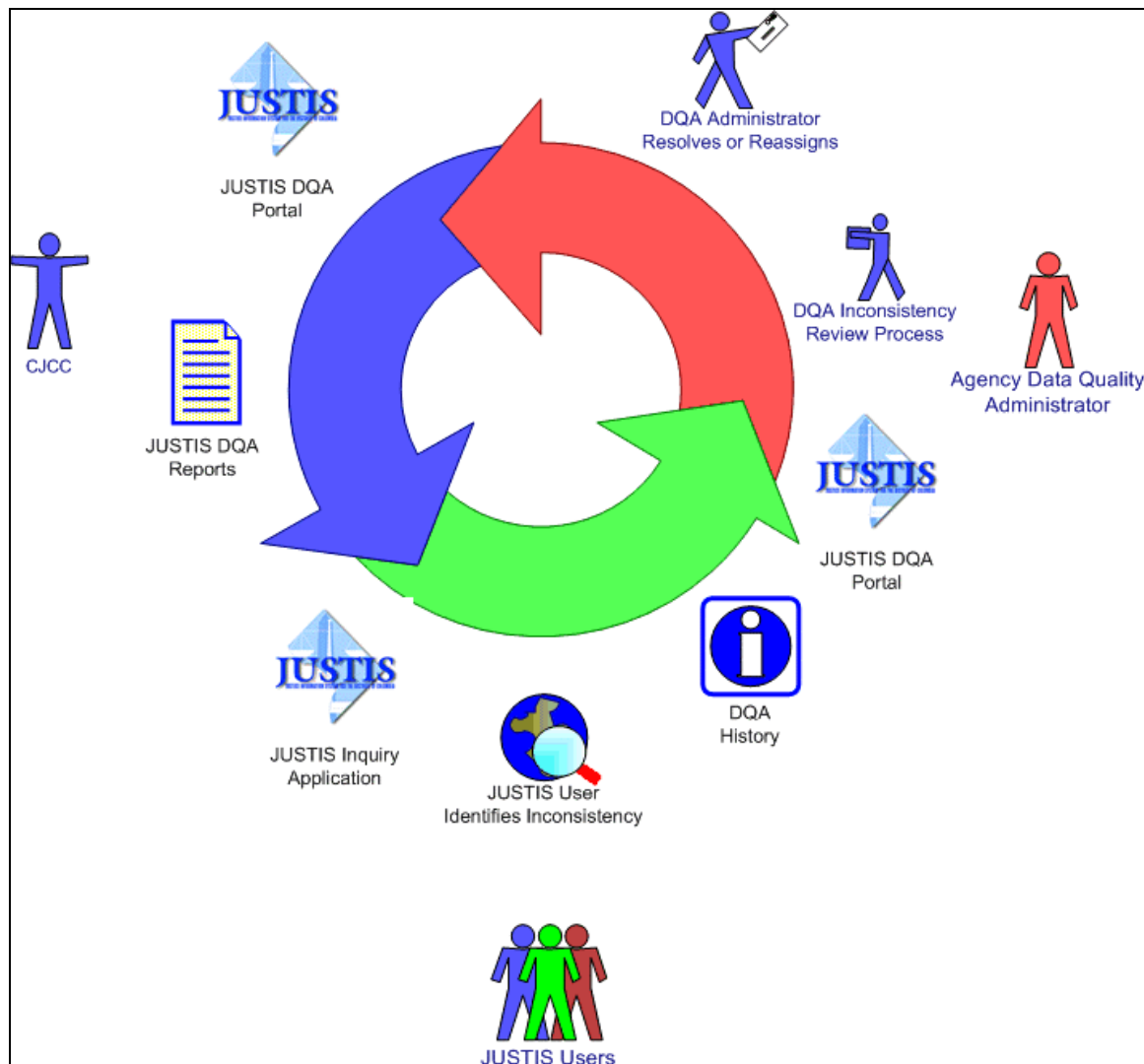


Figure 8 - JUSTIS DQA Business Process

The DQA business process was developed through JAD sessions. The objective of JAD sessions was to establish a set of quality assurance tools that is then made available to all individual users and participating agencies to create a collaborative method of improving actively used records. The DQA tool also creates an audit trail of all questions and changes. The Data Quality Design Document which is part of the JUSTIS documentation further details the business process and the supporting technology that enable the Data Quality Alliance.

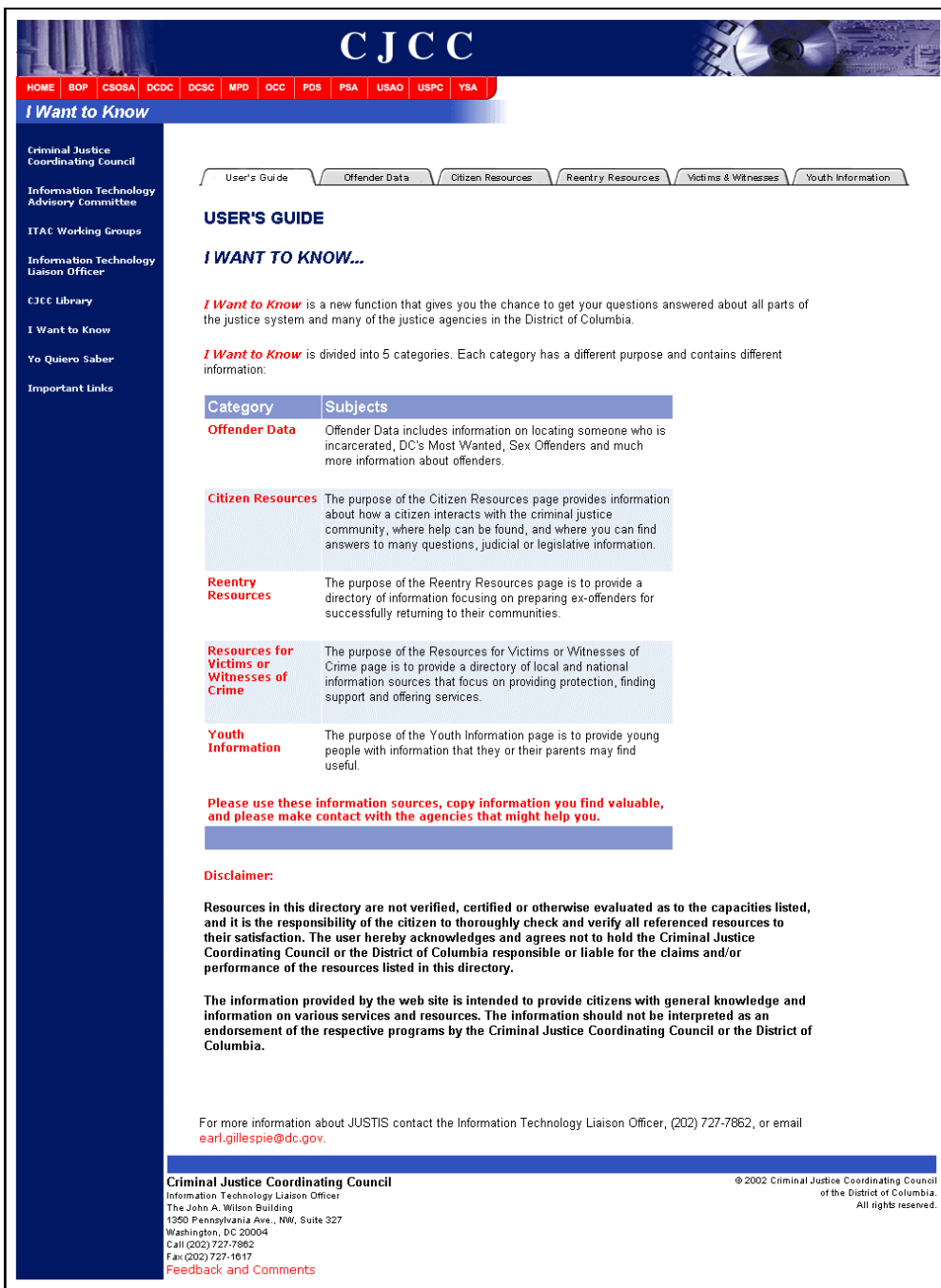
### 3.4.5 *Public Access*

Remaining cognizant of the ITAC guiding principles, JUSTIS provides the opportunity to “nurture agency and community requirements for research and public access.” This principle allows the public to recognize a tangible value from JUSTIS. The methodology for publishing data to the public is completely separate from the primary JUSTIS applications. Located on the District of Columbia DMZ network, the JUSTIS public page ([www.cjcc.dc.gov](http://www.cjcc.dc.gov)) provides a CJCC interface with the public. Data that participating agencies desire to publish on this website can be presented in several formats, including HTML, PDF, or MS Word.

During Phase 3 of JUSTIS development, the CJCC public Internet presence was further enhanced through the development of a set of pages called “I Want To Know...” These pages provide a “one-stop-shop” for public safety information for a variety of groups in the public safety community. These groups range from victims of crimes to at-risk youth.

The “I Want To Know” page links the various groups with numerous online resources publicly available to them. The “I Want To Know...” homepage is pictured below.





**CJCC**

HOME BOP CSOSA CDC DCSC MPD OCC PDS PSA USAO USPC YSA

**I Want to Know**

Criminal Justice Coordinating Council

Information Technology Advisory Committee

ITAC Working Groups

Information Technology Liaison Officer

CJCC Library

I Want to Know

Yo Quiero Saber

Important Links

User's Guide Offender Data Citizen Resources Reentry Resources Victims & Witnesses Youth Information

**USER'S GUIDE**

**I WANT TO KNOW...**

**I Want to Know** is a new function that gives you the chance to get your questions answered about all parts of the justice system and many of the justice agencies in the District of Columbia.

**I Want to Know** is divided into 5 categories. Each category has a different purpose and contains different information:

Category	Subjects
<b>Offender Data</b>	Offender Data includes information on locating someone who is incarcerated, DC's Most Wanted, Sex Offenders and much more information about offenders.
<b>Citizen Resources</b>	The purpose of the Citizen Resources page provides information about how a citizen interacts with the criminal justice community, where help can be found, and where you can find answers to many questions, judicial or legislative information.
<b>Reentry Resources</b>	The purpose of the Reentry Resources page is to provide a directory of information focusing on preparing ex-offenders for successfully returning to their communities.
<b>Resources for Victims or Witnesses of Crime</b>	The purpose of the Resources for Victims or Witnesses of Crime page is to provide a directory of local and national information sources that focus on providing protection, finding support and offering services.
<b>Youth Information</b>	The purpose of the Youth Information page is to provide young people with information that they or their parents may find useful.

**Please use these information sources, copy information you find valuable, and please make contact with the agencies that might help you.**

**Disclaimer:**

Resources in this directory are not verified, certified or otherwise evaluated as to the capacities listed, and it is the responsibility of the citizen to thoroughly check and verify all referenced resources to their satisfaction. The user hereby acknowledges and agrees not to hold the Criminal Justice Coordinating Council or the District of Columbia responsible or liable for the claims and/or performance of the resources listed in this directory.

The information provided by the web site is intended to provide citizens with general knowledge and information on various services and resources. The information should not be interpreted as an endorsement of the respective programs by the Criminal Justice Coordinating Council or the District of Columbia.

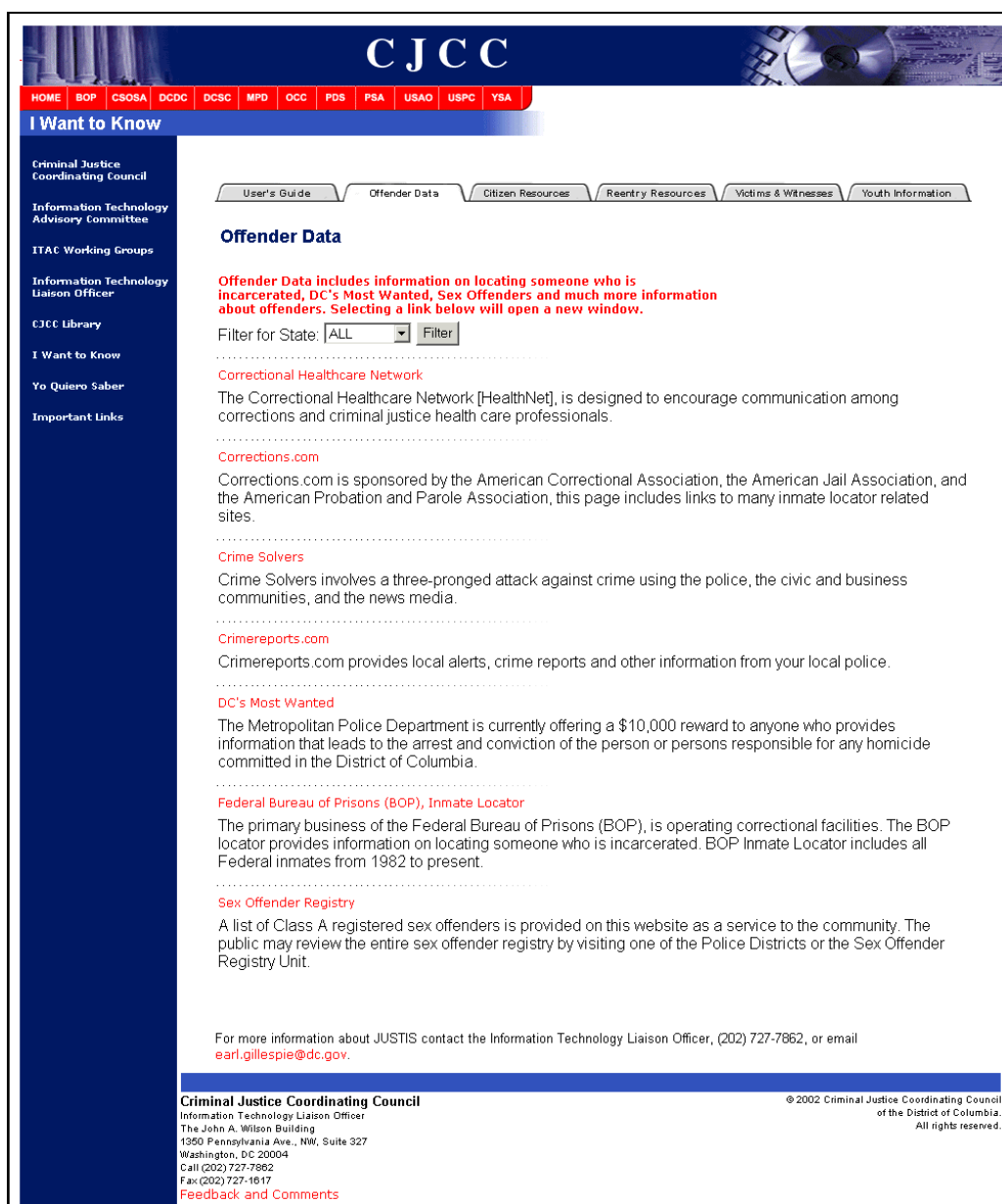
For more information about JUSTIS contact the Information Technology Liaison Officer, (202) 727-7862, or email [earl.gillespie@dc.gov](mailto:earl.gillespie@dc.gov).

**Criminal Justice Coordinating Council**  
Information Technology Liaison Officer  
The John A. Wilson Building  
1350 Pennsylvania Ave., NW, Suite 327  
Washington, DC 20004  
Call (202) 727-7862  
Fax (202) 727-1617  
[Feedback and Comments](#)

© 2002 Criminal Justice Coordinating Council of the District of Columbia. All rights reserved.

Figure 9 - CJCC "I Want To Know..." Homepage

The following picture illustrates the resources that a public user whom is interested in Internet resources available to an Offender via the CJCC "I Want To Know..." page.



**CJCC**

HOME BOP CSOSA DCDC DCSC MPD OCC PDS PSA USAO USPC YSA

**I Want to Know**

Criminal Justice Coordinating Council  
Information Technology Advisory Committee  
ITAC Working Groups  
Information Technology Liaison Officer  
CJCC Library  
I Want to Know  
Yo Quiero Saber  
Important Links

User's Guide Offender Data Citizen Resources Reentry Resources Victims & Witnesses Youth Information

### Offender Data

Offender Data includes information on locating someone who is incarcerated, DC's Most Wanted, Sex Offenders and much more information about offenders. Selecting a link below will open a new window.

Filter for State:

**Correctional Healthcare Network**  
The Correctional Healthcare Network [HealthNet], is designed to encourage communication among corrections and criminal justice health care professionals.

**Corrections.com**  
Corrections.com is sponsored by the American Correctional Association, the American Jail Association, and the American Probation and Parole Association, this page includes links to many inmate locator related sites.

**Crime Solvers**  
Crime Solvers involves a three-pronged attack against crime using the police, the civic and business communities, and the news media.

**Crimereports.com**  
Crimereports.com provides local alerts, crime reports and other information from your local police.

**DC's Most Wanted**  
The Metropolitan Police Department is currently offering a \$10,000 reward to anyone who provides information that leads to the arrest and conviction of the person or persons responsible for any homicide committed in the District of Columbia.

**Federal Bureau of Prisons (BOP), Inmate Locator**  
The primary business of the Federal Bureau of Prisons (BOP), is operating correctional facilities. The BOP locator provides information on locating someone who is incarcerated. BOP Inmate Locator includes all Federal inmates from 1982 to present.

**Sex Offender Registry**  
A list of Class A registered sex offenders is provided on this website as a service to the community. The public may review the entire sex offender registry by visiting one of the Police Districts or the Sex Offender Registry Unit.

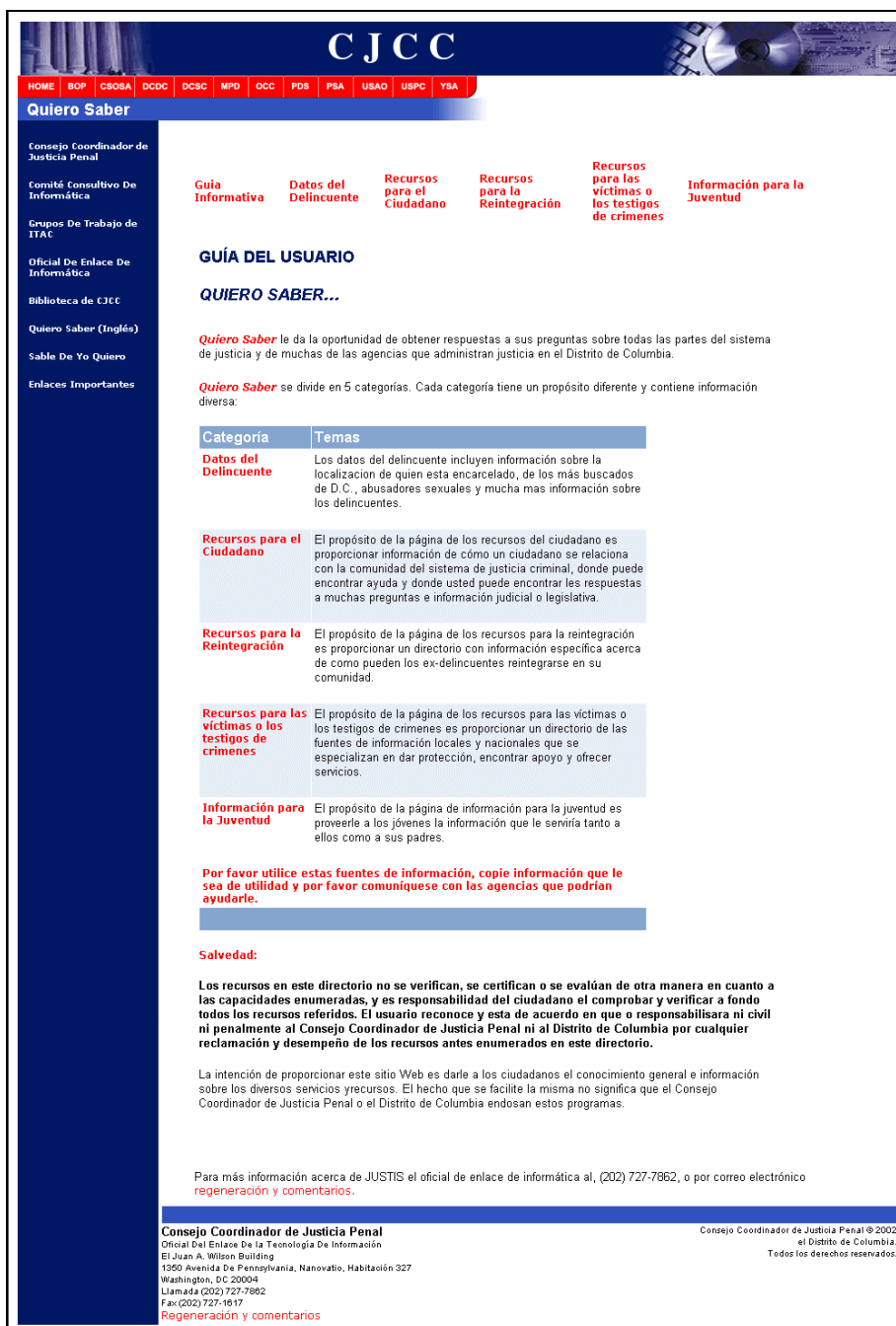
For more information about JUSTIS contact the Information Technology Liaison Officer, (202) 727-7862, or email [earl.gillespie@dc.gov](mailto:earl.gillespie@dc.gov).

**Criminal Justice Coordinating Council**  
Information Technology Liaison Officer  
The John A. Wilson Building  
1350 Pennsylvania Ave., NW, Suite 327  
Washington, DC 20004  
Call (202) 727-7862  
Fax (202) 727-1617  
[Feedback and Comments](#)

© 2002 Criminal Justice Coordinating Council of the District of Columbia. All rights reserved.

Figure 10 - CJCC "I Want To Know..." Offender Data

The CJCC "I Want To Know..." page has been further enhanced with the translation of this public resource into Spanish. The picture below illustrates the "Yo Quiero Saber..." homepage, thus providing the same valuable resource to a community that had been underserved. It is important to note that the homepage only is translated into Spanish, once the user follows the hyperlink by clicking on it; it is the responsibility of the resource owner to translate the page.



**CJCC**

HOME BOP CSOSA DCDC DCSC MPD OCC PDS PSA USAO USPC YSA

**Quiero Saber**

Consejo Coordinador de Justicia Penal  
Comité Consultivo De Informática  
Grupos De Trabajo de ITAC  
Oficial De Enlace De Informática  
Biblioteca de CJCC  
Quiero Saber (Inglés)  
Sabe De Yo Quiero  
Enlaces Importantes

**Guía Informativa** **Datos del Delincuente** **Recursos para el Ciudadano** **Recursos para la Reintegración** **Recursos para las víctimas o los testigos de crímenes** **Información para la Juventud**

**GUÍA DEL USUARIO**

**QUIERO SABER...**

**Quiero Saber** le da la oportunidad de obtener respuestas a sus preguntas sobre todas las partes del sistema de justicia y de muchas de las agencias que administran justicia en el Distrito de Columbia.

**Quiero Saber** se divide en 5 categorías. Cada categoría tiene un propósito diferente y contiene información diversa:

Categoría	Temas
<b>Datos del Delincuente</b>	Los datos del delincuente incluyen información sobre la localización de quien está encarcelado, de los más buscados de D.C., abusadores sexuales y mucha más información sobre los delincuentes.
<b>Recursos para el Ciudadano</b>	El propósito de la página de los recursos del ciudadano es proporcionar información de cómo un ciudadano se relaciona con la comunidad del sistema de justicia criminal, donde puede encontrar ayuda y donde usted puede encontrar las respuestas a muchas preguntas e información judicial o legislativa.
<b>Recursos para la Reintegración</b>	El propósito de la página de los recursos para la reintegración es proporcionar un directorio con información específica acerca de cómo pueden los ex-delincuentes reintegrarse en su comunidad.
<b>Recursos para las víctimas o los testigos de crímenes</b>	El propósito de la página de los recursos para las víctimas o los testigos de crímenes es proporcionar un directorio de las fuentes de información locales y nacionales que se especializan en dar protección, encontrar apoyo y ofrecer servicios.
<b>Información para la Juventud</b>	El propósito de la página de información para la juventud es proveerle a los jóvenes la información que le serviría tanto a ellos como a sus padres.

**Por favor utilice estas fuentes de información, copie información que le sea de utilidad y por favor comuníquese con las agencias que podrían ayudarlo.**

**Salvedad:**

Los recursos en este directorio no se verifican, se certifican o se evalúan de otra manera en cuanto a las capacidades enumeradas, y es responsabilidad del ciudadano el comprobar y verificar a fondo todos los recursos referidos. El usuario reconoce y está de acuerdo en que o responsabilizará ni civil ni penalmente al Consejo Coordinador de Justicia Penal ni al Distrito de Columbia por cualquier reclamación y desempeño de los recursos antes enumerados en este directorio.

La intención de proporcionar este sitio Web es darle a los ciudadanos el conocimiento general e información sobre los diversos servicios y recursos. El hecho que se facilite la misma no significa que el Consejo Coordinador de Justicia Penal o el Distrito de Columbia endosan estos programas.

Para más información acerca de JUSTIS el oficial de enlace de informática al, (202) 727-7862, o por correo electrónico [regeneración y comentarios](#).

**Consejo Coordinador de Justicia Penal**  
Oficial Del Enlace De la Tecnología De Información  
El Juan A. Wilson Building  
1350 Avenida De Pennsylvania, Nanavatio, Habitación 327  
Washington, DC 20004  
Llamada (202) 727-7862  
Fax (202) 727-1617  
[Regeneración y comentarios](#)

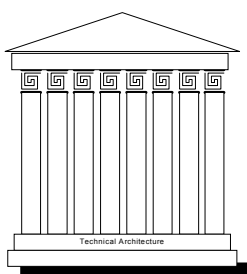
Consejo Coordinador de Justicia Penal © 2002  
el Distrito de Columbia.  
Todos los derechos reservados.

Figure 11 - CJCC "Yo Quiero Saber..." Homepage

The final benefit that has been enabled with the development and deployment of the CJCC public presence is the accessibility provided to those with disabilities, such as

blindness. Again, this is providing this valuable public resource to a community of users that had been previously underserved.

## 3.5 Technical Architecture



We have discussed the overall business requirements and system goals of JUSTIS. We then discussed the functional elements of the systems that collectively empowered JUSTIS users to achieve the business objectives. This section now turns to the technical infrastructure and architecture necessary to support the functional elements.

### 3.5.1 *Full Security Implementation*

The JUSTIS security architecture is modeled after the World Wide Web. Information to be shared is “published” by its owner agency on distributed JUSTIS Agency Servers, and authorized agency personnel can access JUSTIS server content using web-browser software on a desktop computer. A Hub Server provides a shared platform for centralized applications, agency-independent content, and inter-agency communication.

Unlike the web, however, JUSTIS is a secure Intranet. Firewalls protect the network from unauthorized access. Digital certificates and Intranet data encryption provides secure communication and user/server authentication.

The JUSTIS network provides a cooperative and collaborative environment in which many users of the network are interacting at any given time. This interaction requires a strong and flexible layer of security to provide protection to communications over the network and to data stored on the legacy systems.

Security is a collection of technologies and policies that enable JUSTIS to provide and deny access to system resources on a controlled and consistent basis. Security protects the system resources, which can be either physical (network) or informational (application).

The design of the JUSTIS security implementation is fully documented in two deliverables presented during the course of JUSTIS Phase 3. The first, deliverable number 1.10 Security Policy and Procedures, provides an overview of

the security policies and procedures that are the foundation upon which JUSTIS operates. This document conveys the importance of a hierarchical organizational structure in the administration of system security, provides an administrative policy, and concludes with a user access policy. Also included in the deliverable is the necessary user access forms followed by a user agreement and an access flow chart.

The second document that addresses the JUSTIS security implementation is deliverable number 1.13 JUSTIS Security Architecture. This deliverable addresses the technical architecture that contributes to the security implementation. It provides the user with an understanding of the objectives of the JUSTIS Security Architecture and the design and implementation of the full solution. The document communicates this through discussions of security architecture strategies, an evaluation of possible security compromising tactics and their defense, and concludes with security recommendations specific to JUSTIS along with a summary of the current solution.

### *3.5.2 Overall JUSTIS Building Blocks: Web Application Development Standards*

As stated in the beginning of this Blueprint, a business requirement of JUSTIS is that it be built upon open standards and technologies. This requirement demands an approach that uses internationally accepted standard tools and techniques. Such tools are available from a wide variety of vendors. Systems developed with open technologies run on a wide variety of platforms.

The use of open technologies is important to the District and to the success of JUSTIS. Open technologies offer a number of advantages:

**Vendor neutrality.** Developers who employ open standards technologies avoid locking themselves into a single vendor. This reduces project risk because a single vendor can fail to fix bugs, slip on release dates or go out of business altogether.

**Platform independence.** Systems that are developed on open standards technologies are easier to move from one hardware platform to another or from one operating system to another.

**Greater flexibility.** Because of vendor neutrality and platform independence, JUSTIS participating agencies will have fewer concerns about upgrading their systems and changing platforms. A JUSTIS component built to run on Windows NT and connect to a SQL Server database will require only small modifications to run on a UNIX platform connecting to an Oracle database.

During the POC phase, the JUSTIS team developed the system under the Java 2 Enterprise Edition (J2EE) set of standards. The standards selected within this framework were all at an accepted level – no draft standards or vendor extensions were employed.

The specific standards used to develop and deploy JUSTIS POC System code were:

**JDK 1.3** – The Java Development Kit, the Java programming language system used to develop JUSTIS application code.

**Java Servlets 2.1** – Servlets are Java code that runs under the control of JUSTIS web servers.

**JSP 1.0** – Java Server Pages are server-processed web pages that include programmatic Java elements.

**JDBC 2.0** – JDBC is the standard access method that connects JUSTIS Java programs with back-end databases.

**XML and XSLT 1.0** – The Extensible Markup Language and its accompanying style sheet language is a bundle of several related technologies. In JUSTIS, they are used to extend the power of basic web HTML pages.

**TCP/IP** – Transmission Control Protocol/Internet Protocol. TCP/IP is a family of communications protocols that control traffic across the DC Wide Area Network.

**HTML 3.2** – The Hypertext Markup Language is what web pages are written in. The version 3.2 standard has been used to help ensure maximum browser independence.

**HTTP 1.1/1.0 Hypertext Transfer Protocol** – This is the standard protocol for transmitting information between browsers and servers. HTTP is a layer above TCP in the protocol stack.

**SSL 3 – Secure** Sockets Layer version 3. SSL enables HTTP and other protocols to be transmitted in encrypted form across a network.

**X.509v3** – ITU-T Recommendation X.509 defines an authentication framework based on digital certificates. The recommendation specifies a set of properties and content for digital certificates, as well as procedures for authentication and certificate management.

**X.500 Directory Services** – X.500 is the standard for Directory Services. Directories are essentially databases optimized for read-access of network entity information. JUSTIS uses an X.500 based directory to store information about users, servers, and

applications – including group membership and digital certificates – in a centralized location. The Directory Service is available to applications such as web servers and browsers that require identifying information about an entity in JUSTIS. A prime example is a web server that assigns access control to web resources based on group memberships defined in the directory.

**LDAP Lightweight Directory Access Protocol** – LDAP is a protocol used by applications to communicate with the Directory. Applications are expected to utilize LDAP and the Directory to reduce the redundancy of user information on systems in a network environment.

**SMTP, S/MIME, POP3 and IMAP4.** – These protocols collectively provide a secure email environment.

During Phase 2 development, the ITAC TWG and OCTO representatives reviewed the standards used throughout the District. It was discovered that in all justice agencies, as well as in the majority of other city agencies, the server application platform most widely used for deployment was Microsoft (MS). No substantial J2EE systems, other than the JUSTIS POC, were deployed in the District in the Spring of 2001.

As a further part of this analysis, OCTO and the JUSTIS implementation team performed a cost benefit comparison of continuing with a J2EE path versus standardizing on Microsoft. This comparison showed that an MS server deployment would be less expensive than J2EE.

Therefore, recognizing that MS was the preferred platform in the justice community and other city agencies, recognizing that an MS deployment would be more cost-effective, and recognizing that agency participation in JUSTIS would be easier if JUSTIS used the same technologies already in use at the agencies, the ITLO and OCTO decided to refine the set of standards used in JUSTIS to incorporate certain MS technologies.

This decision had the following impact on Phase 2. First, there are a number of technologies that were used in the development of the JUSTIS POC that will continue to be the standard for JUSTIS Phase 2. These are:

JUSTIS POC, Phase 2, and Phase 3 Architecture Standards	
Category	Product/Standard
Operating System	MS Windows 2000 Advanced Server
Directory Services	MS Windows 2000 Active Directory

JUSTIS POC, Phase 2, and Phase 3 Architecture Standards	
Category	Product/Standard
Web Server	MS Internet Information Server 5
Web Browser	Either IE5 or NS5 or above
Browser scripting	JavaScript and VBScript
Browser markup	HTML 3.2 and Adobe PDF
Database	MS SQL Server 2000
Web Page Design	Macromedia UltraDev DreamWeaver

Secondly, a number of standards used for the POC were changed for JUSTIS Phase 2 and subsequent phases. These standards are:

Category	Phase 2 and Phase 3 Standards	POC Standard
Server scripting	MS ASP	Sun JSP
Server objects	MS VB COM, WebClasses	Sun Servlets
Application Server	MS IIS 5	Allaire Jrun
Database drivers	MS ODBC	Various JDBC
Development Suite	MS Visual Studio	Inprise Visual Studio

This change is to ease the impact that participation in JUSTIS has on its member agencies. The change to certain MS technologies assists member agencies in leveraging staff skills and software components that are already in place.

The change to server component standards does not change the basic tenet of JUSTIS to deploy open standards wherever possible. The bulk of the standards used, especially at the user interface tier, remain the internationally ratified standards. A description of the 3-Tier model JUSTIS uses and the standards in place at each tier follows.

The JUSTIS system is created on according to a classic 3-Tier paradigm. Systems built along this model are inherently more maintainable because they



are functionally organized into modular components that can be individually maintained. The 3-Tiers are the user interface tier, the business logic tier and the backend database tier.

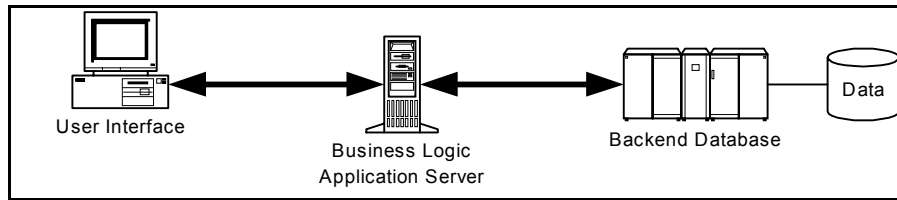


Figure 12– Three Tier Architecture

The user interface tier accepts users input (keystrokes and mouse clicks) and displays user output to the screen. In the JUSTIS model, the user interface tier is a standard web browser. Any web browser that can support HTML 3.2 will be able to use JUSTIS. Additional functionality may be delivered to web browsers that are capable of running Java applets, JavaScript and DHTML. Generally, Netscape version 4 and above and Microsoft Internet Explorer version 4 and above workstations will be able to use JUSTIS.

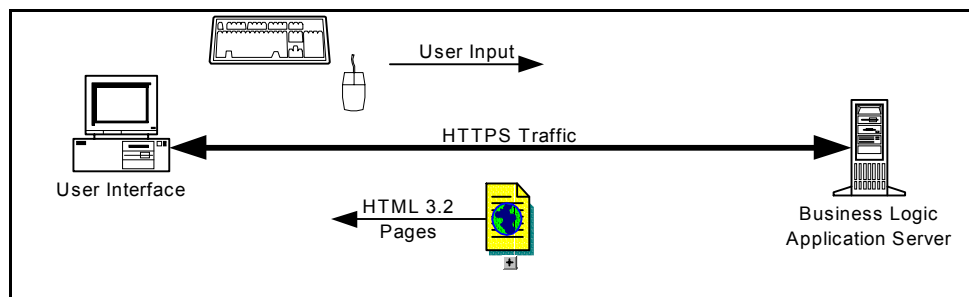


Figure 13– Communication between User Interface and Business Logic Tiers

The business logic tier in JUSTIS is a standard web server that delivers standard web pages to the user interface tier. The business logic is built using Active Server Pages and ODBC connections to the data tier. JUSTIS is built using Microsoft IIS web server.

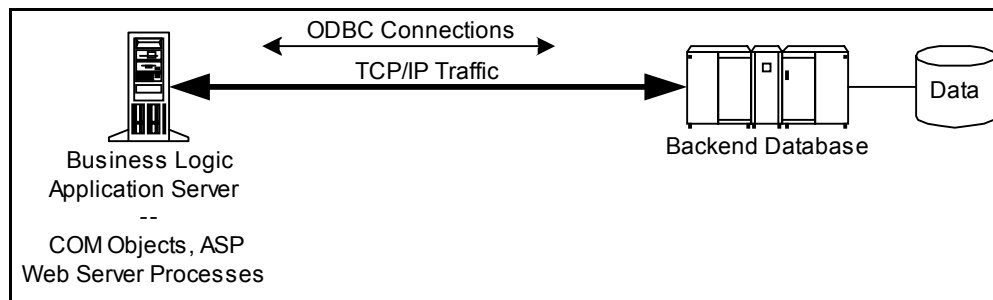


Figure 14– Communication between Business Logic and Backend Database Tiers

The backend data tier is under the control of the participating JUSTIS agency. The use of open standards means that this tier can change with minimal impact on the system. For example, should the database change from SQL Server to Oracle, only one line of code needs to change – the one that makes the ODBC connection

### 3.5.3 *Physical Plant Design of JUSTIS Components*

#### 3.5.3.1 Overall Architecture

The overall JUSTIS network is a hub and spoke architecture. The hub components, described below, serve as a centralized traffic manager and offer enterprise-wide services such as email, security certificates, discussion group management and directory services.

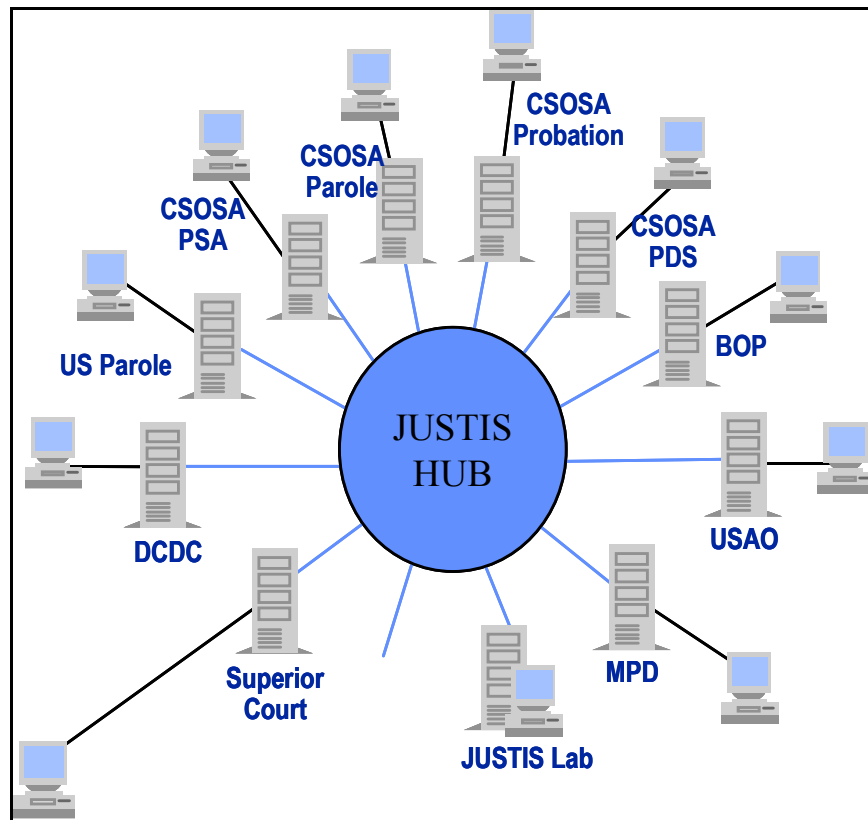


Figure 15– JUSTIS Hub and Spoke Structure

The spokes of the network are participating agency servers connected to the agency's network, user workstations, and legacy applications and data. Connections are through the DC Wide Area Network using the TCP/IP protocol.

The standards used in the design of JUSTIS leave flexibility in the selection of hardware and software. The details in this section show hardware and software choices that will be compatible with the JUSTIS architecture, but they should not be viewed as absolute requirements.

The server hardware that supports each Hub server as well as each agency server is summarized in the following table:

JUSTIS Typical Server Configuration	
Processor:	933MHz x2 w/256 cache
Memory:	1024 MB
	36GB x 3 in RAID 5 configuration

JUSTIS Typical Server Configuration	
RAID 5 SCSI Adapter	
Storage Device: 20/40 GB DLT Tape Drive	
Network Services: 1 – Compaq Netflex3 10/100 Embedded NIC Adapter	
Power Supplies (2)	
Processor: 933MHz x2 w/256 cache	
Memory: 1024 MB	
36GB x 3 in RAID 5 configuration	
RAID 5 SCSI Adapter	
Storage Device: 20/40 GB DLT Tape Drive	
Network Services: 1 – Compaq Netflex3 10/100 Embedded NIC Adapter	
Power Supplies (2)	
Processor: 933MHz x2 w/256 cache	
Warranty : 3 Year Limited Warranty	

### 3.5.3.2 JUSTIS HUB Components

The Hub of JUSTIS contains the following servers:

**Discussion Group Server** – this server provides central support for NNTP services. It supports JUSTIS discussion groups.

**Certificate Server** – this server is used to assign and maintain security certificates.

**Directory Server** – this server supports LDAP directory services. It stores user login information, security certificates, email addresses and other directory information.

**Central Web Server** – The home page of JUSTIS resides on this server. This server serves as a central launching point for the inquiry applications, email, and access to agency web servers and discussion groups. It also provides indexed search of HTML pages and reference libraries on the JUSTIS web and agency servers, as well as

search of Internet resources and static web page content such as JUSTIS news, policies, and procedures.

The software components for these servers are:

Component	Standards/Protocols	Product
Web Server	HTTP, HTML	MS IIS V 5
Mail Server	SMTP, S/MIME	MS Exchange Server
Directory Server	LDAP, LDAP API	Microsoft Active Directory
Discussion Group	NNTP	Netscape Collabra
Certificate Server	X.509v3	X.509 Verisign

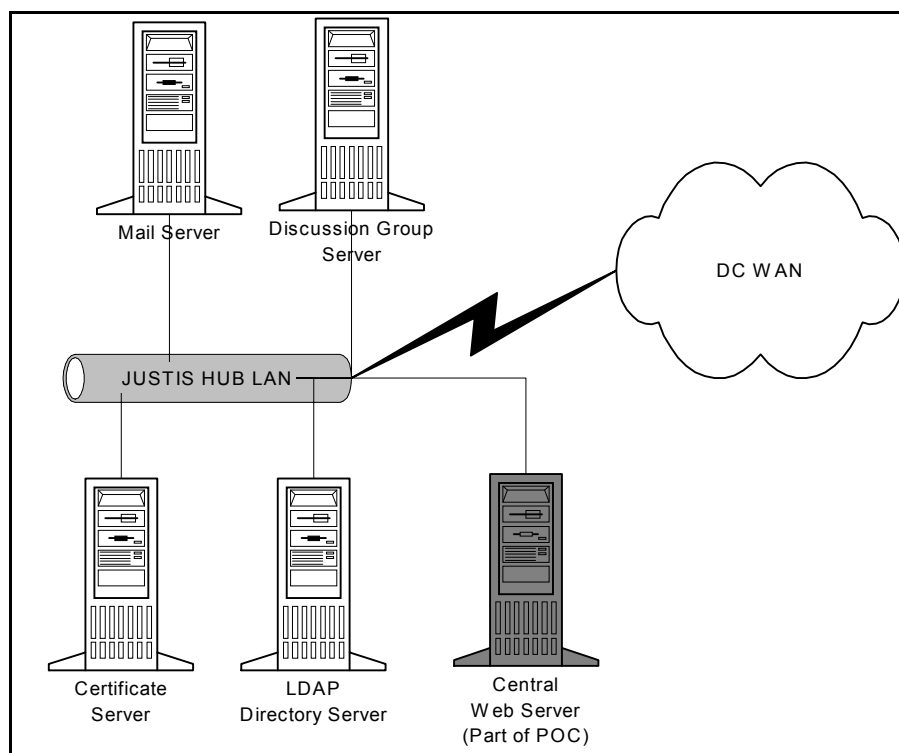


Figure 16– JUSTIS Hub Components

### 3.5.3.3 JUSTIS Agency Components

A number of the participating JUSTIS agencies contain one server:

**Agency FTP Server (if applicable)** – The File Transfer Protocol (FTP) Server provides a host to receive and transmit files via file transfer protocol. Due to the secure nature of the data being transmitted to the JUSTIS infrastructure, WS\_FTP is the FTP server of choice.

The software components for this server are:

Component	Standards/Protocols	Product
FTP Server	128 bit encrypted SSL File Transfer Protocol	IPSwitch WS_FTP Server

### 3.5.4 Scalability, Performance Requirements

The JUSTIS proof-of-concept system was required to support fewer than 40 users. However, the design and implementation will allowed for scaling to hundreds or thousands of users. During JUSTIS Phase 2 the infrastructure was expanded to support up to 2,000 users.

Further scalability and performance improvements can be implemented on different components, these are discussed below.

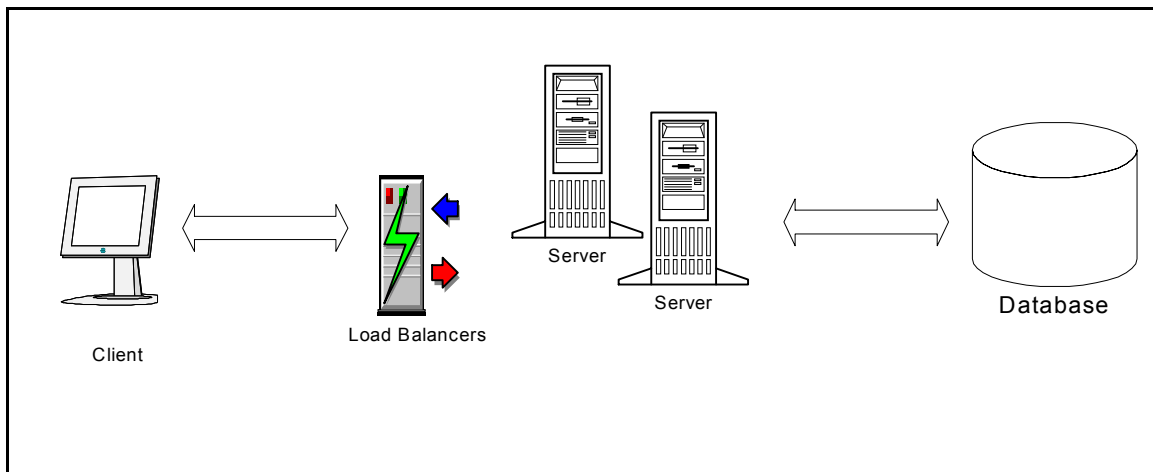


Figure 17– Areas to Examine for Performance Improvements

Component	Optimizing Technique
Client Side	On the client side, the power of the workstation can be improved by increasing the memory and the processor speed. The disk can be defragmented and the file system optimized
Load Balancers	Load balancers are used between the client and the server, so that the load is distributed equally among multiple servers.
Server	The server side performance improvements can be done be using Servlets and JSP technologies that uses only one active connection to the database for processing the clients request. The use of distributed computing environment increases the performance and scalability to a large extent.

Component	Optimizing Technique
	Java code can be written to be multi-threaded and to take advantage of multiple processors.
Database	By creating additional indexes on the tables that are queried frequently will improve the performance. Also by running the database in multi-threaded mode will improve performance.
Network	A better network infrastructure will improve the end-to-end response time. Higher speed LAN connections as well as WAN connections can be employed.

### 3.5.5 User Workstations

JUSTIS is a browser-based application; therefore, the system has been developed to work effectively with the following components:

- **Network** – Currently the JUSTIS POC is hosted by the District of Columbia’s Office of the Chief of Technology Officer (OCTO), therefore users of the system must have a connection to the District of Columbia’s Wide Area Network in order to gain access to the system. Similarly, if it is determined to develop JUSTIS on a separate wide area network, all users must have access to the network.
- **Browser** – Internet Explorer 4.0 or higher or Netscape Navigator 4.0 or higher. JUSTIS works most effectively with Internet Explorer, due to techniques employed in the District of Columbia OCTO Web Development Kit.
- **Computer Processor** – 486DX/66 MHz or higher processor.
- **Operating System** – Windows ME, Windows 95, Windows 98, Windows 2000, or Windows NT 4.0.
- **Memory** – For Windows 95, Windows 98, and Windows 2000: 16 MB (megabytes) of RAM minimum. For Windows NT: 32 MB of RAM minimum.
- **Screen Resolution** – JUSTIS is designed to be operational at all screen resolutions. A minimum resolution of 800 by 600 provides the most effective usage without the need for horizontal scrolling.

As stated before, JUSTIS is designed to be a secure intranet. This requires security components in a browser that may not be included in the version currently residing on a users’ system. The users’ browser is required to have



128-bit encryption strength. Future JUSTIS functionality may require cookies or JAVA applets.

### *3.5.6 Network Infrastructure: Special Security Considerations*

Security infrastructure is documented in JUSTIS Phase 2 deliverable 1.1.2, JUSTIS Security Architecture, which was completed during Phase 2. This document provides readers with an understanding of the objectives of the JUSTIS security architecture and illustrates the design and implementation of a full security solution. It accomplishes this by explaining security architecture strategies, security compromising tactics and their defense, and concludes with a recommendation of a full security solution specifically for JUSTIS.

### *3.5.7 Application Development Guidelines*

JUSTIS was developed using contemporary Internet technologies. The specific components used to develop applications associated with JUSTIS are documented in JUSTIS Phase 2 deliverable 1.11, JUSTIS Programming Guide. This deliverable outline the Visual Basic programming styles used throughout Phase 2 by providing a basic understanding of the structure, foundation and standards characteristic of the selected standard. It also details the utilization of webclasses throughout Phase 2, by describing the overall architecture of the objects.

### *3.5.8 Off-line, Replicated, Screen-scraped and On-line Data*

Acknowledging that each justice agency is independent, it is assumed that each agency's information infrastructure and management is different. These two facts plus the additional fact that the majority of agencies manage a unique legacy system could provide an obstacle when implementing a common information system across the justice agencies. The problem centers around how will JUSTIS obtain the agreed upon shared information from the legacy system. The JUSTIS architecture provides four paradigms to choose from in order to accommodate access to agency data.

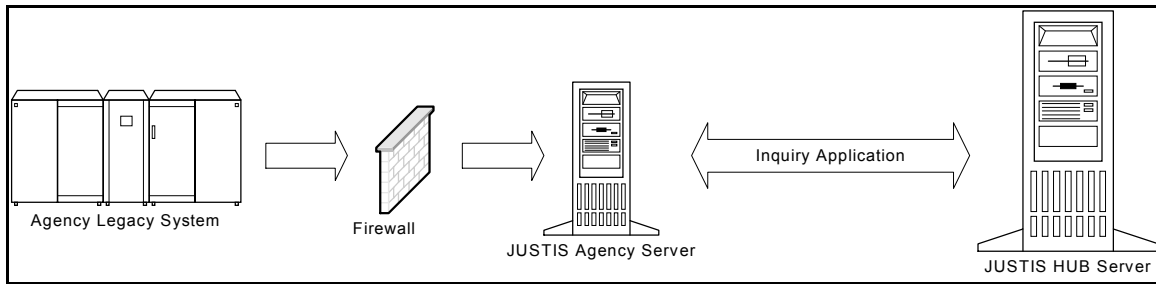


Figure 18– Direct Access

1. JUSTIS can obtain data by directly accessing, in a read-only fashion, that agency's RDBMS database. This would provide the authorized users of the system real-time data retrieval.

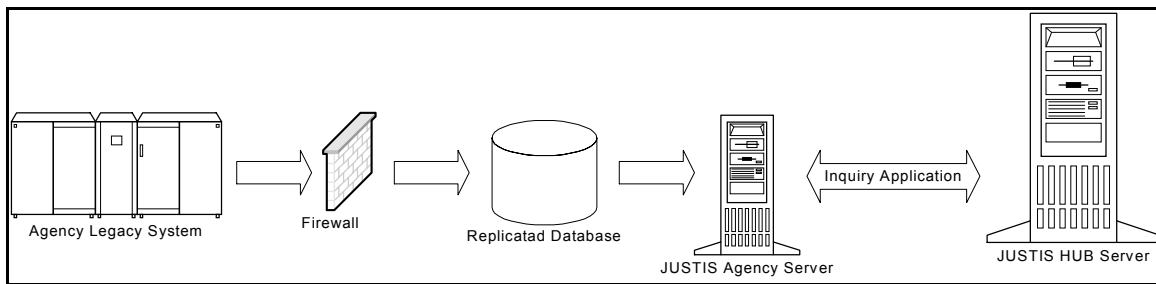


Figure 19– Replicated Access

2. JUSTIS can obtain data by accessing an agency provided replicated database. The data would be updated based upon the programmed schedule of the replicated database.

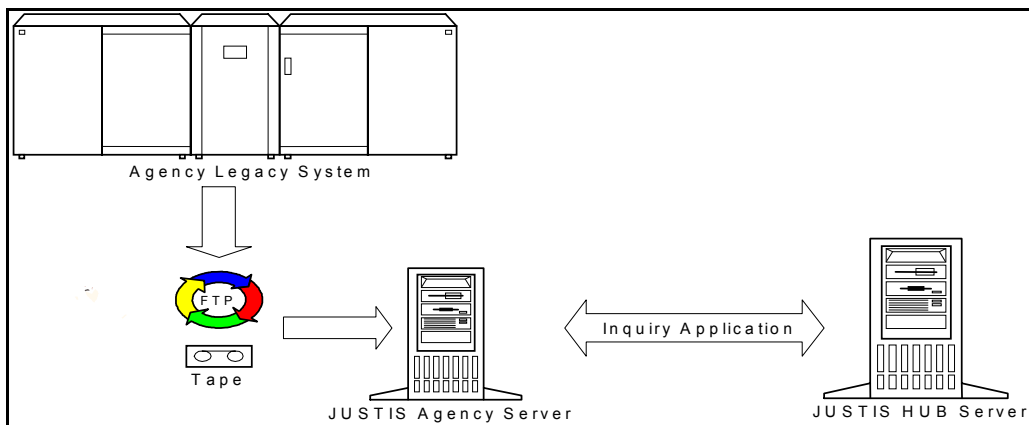


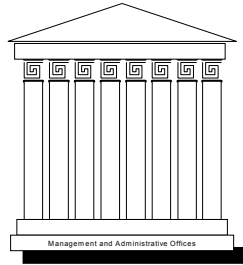
Figure 20– Off-line Access

3. JUSTIS can receive data in an off-line fashion. The data can be downloaded to tape of CD or in FTP format and loaded to the JUSTIS Agency Server. This is the most manual of the three options. This option requires active management of the data transfer. Without active management, data could become outdated, hence ineffective.

4. Finally, the agency legacy systems can be accessed in a screen-scraping fashion. In this scenario, the JUSTIS legacy connection adapter acts as if it were an on-line user of the system. The adapter sends keystrokes to the legacy application and retrieves the resulting screens. These screens are then deconstructed (“scraped”) and the information is transformed into a fashion suitable for use throughout the remainder of the system.

Data Access Method	Pros	Cons
Direct Access	Real-time Data Retrieval Minimal hardware required Minimal software required	Possible legacy system performance impact Possible legacy system security impact
Replicated Data Access	Data is current Lower performance impact Lower security impact	Higher hardware and software costs Need to maintain data extract programs
Off-line Access	Lowest performance impact Lowest security impact	Data is not current Higher hardware and software costs Possible labor-intensive manual processes
Screen Scraping	Real-time data retrieval Legacy data can be in a proprietary format	Costly hardware, software and staff skills required Maintenance intensive Possible performance impact Possible security impact

## 3.6 Management and Administrative Structure



We have discussed the overall mission and business objectives of JUSTIS. We then discussed the functional elements of the system that collectively empower JUSTIS users to achieve the business objectives. The previous section detailed the technical infrastructure and architecture necessary to support the functional elements. We now turn to the bedrock of our future JUSTIS Blueprint – the administrative office structure required to support, maintain, enhance and promote the use of the system.

### 3.6.1 *JUSTIS Organization Chart*

The complete vision for JUSTIS management and administrative structure can be summarized in the following organization chart:

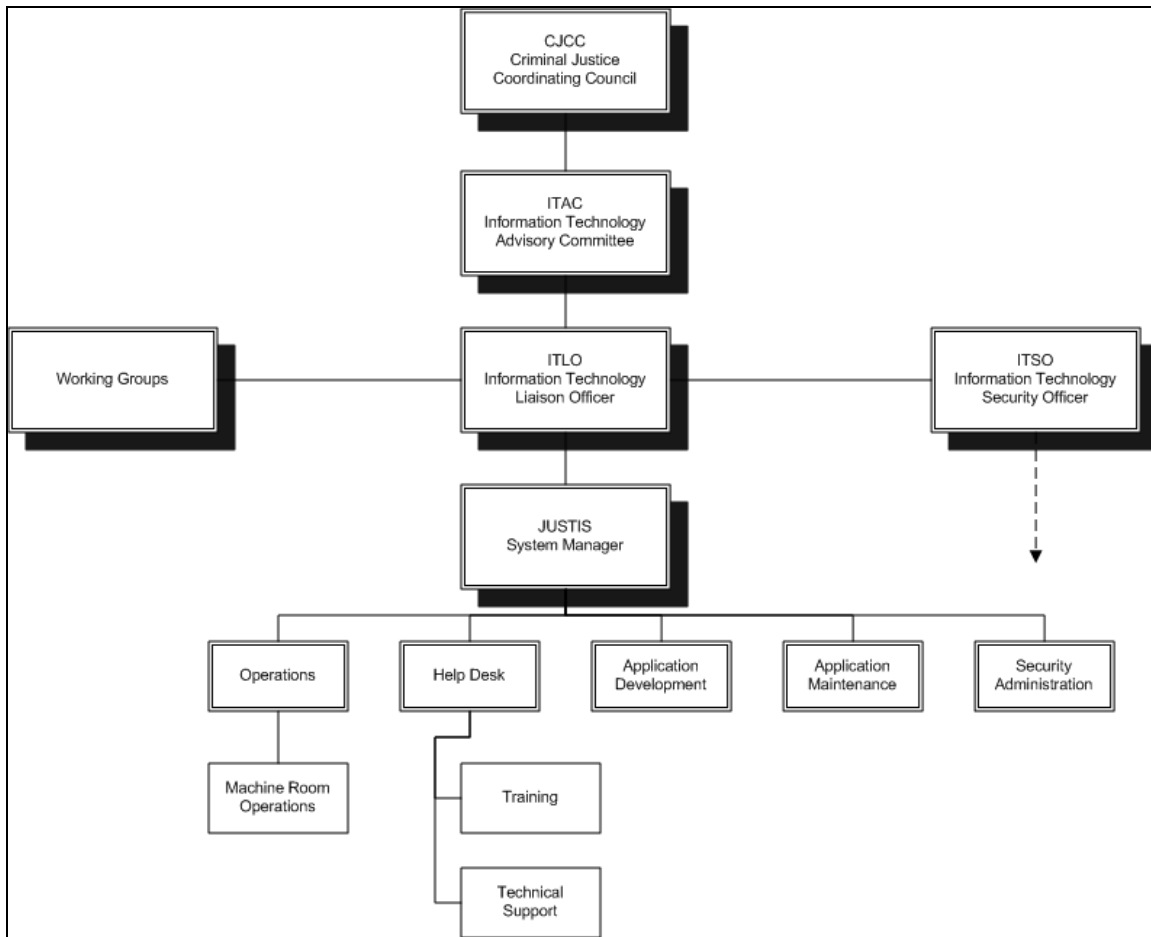


Figure 21– JUSTIS Organization Chart

The roles and responsibilities of the all of the above organizational units and individual members of at operational level are summarized as follows. These member roles and responsibilities are as they relate to JUSTIS – members of the larger organizational units, CJCC and ITAC, having a multitude of additional responsibilities outside of JUSTIS. The individual positions are JUSTIS dedicated personnel.

### 3.6.1.1 CJCC

The CJCC mission statement:<sup>3</sup>

The mission of the Criminal Justice Coordinating Council (CJCC) is to serve as the forum for identifying issues and their solutions, proposing actions, and facilitating cooperation that will improve public safety and the related criminal and juvenile justice services for District of Columbia residents, visitors, victims, and offenders. The CJCC draws upon local and federal agencies and individuals to develop recommendations and strategies for accomplishing this mission. Our guiding principles are creative collaboration, community involvement, and effective resource utilization. We are committed to developing targeted funding strategies and comprehensive management information through integrated information technology systems and social science research in order to achieve our goal.

One of the responsibilities of CJCC in conducting its mission is to set the overall direction and mission for ITAC. The CJCC sets ITAC information technology mission for intra-justice agency collaboration.

### 3.6.1.2 ITAC

#### Mission

The Information Technology Advisory Committee shall advise and recommend on matters pertaining to the funding, development, operation, maintenance and monitoring of a Justice Information System to improve public safety and the related criminal and juvenile justice services for the District of Columbia residents, visitors, victims and offenders.

Recognizing the need for "...comprehensive management information through integrated information technology systems..." the Interagency Agreement established an information Technology Advisory Committee (ITAC) to serve as the governance body for system development. The Interagency Agreement also established a set of guiding principles:

- Recognize the primacy of each justice agency mission
- Facilitate collaborative solutions to justice information challenges
- Commit to the quality and integrity of justice data

---

<sup>3</sup> See [HTTP://WWW.CJCCDC.ORG](http://www.cjccdc.org)

- Implement effective data and system security
- Respect the confidentiality of information and individual privacy
- Establish of system-wide standards, supported by common identifiers and positive identification
- Nurture agency and community requirements for research and public access
- Provide for long term performance monitoring and evaluation

The mission of the ITAC is to advise and make recommendations to the CJCC on matters pertaining to the funding, development, operation, maintenance, and monitoring of a Justice Information System which will help improve public safety and the related criminal and juvenile justice services for the District of Columbia residents, visitors, victims and offenders. The ITAC hired an Information Technology Liaison Officer (ITLO) to serve as the motivator, facilitator, and manager of system development.

In effect, the ITAC carries out the mission it is given by CJCC and has the responsibility to:

- Identify the community expansion of JUSTIS participants
- Identify the functional expansion of JUSTIS capabilities
- Prioritize the order of implementation of the above expansions
- Manage, Control and Monitor the implementation of JUSTIS

### **3.6.1.3 Information Technology Liaison Officer (ITLO)**

The ITAC requires staff resources to for the practical day-to-day administrative activities of the Committee. This staff resource must also function as an ombudsman and liaison between the ITAC; the Executive Director of the Criminal Justice Coordinating Council, Working Group Chairs, and agencies which provide and procure fiscal and technical support such as OGMD, OCTO, the CFO and CPO. The ITLO will also communicate directly with justice agency personnel. The ITLO serves as the manager of system planning and development.

**Goals**

Establish central information systems communications methodology and facility for the justice community

Coordinate and promote funding and technical assistance for all aspects of Justice Information System analysis, documentation, design, and implementation

Provide liaison and coordination between agency program managers, justice agencies and financial and technical agencies, city and Federal levels of government, and the Executive and Judicial branches

Document, monitor, and report the status of both long and short term project efforts

Support the activities of all Working Groups and Subcommittees established by the ITAC

Establish a DC justice documentation archive including the Justice Data Dictionary and maintain such documentation and systems as identified by the ITAC

**Objectives**

Coordinate funding and technical assistance from OGM, OCTO, the CFO, the CPO, BJS and BJA, and other appropriate individuals, organizations and government programs

Manage the technical assistance resources

Identify and recommend the establishment or termination of Working Groups and Subcommittees to the ITAC

Recommend chairs and membership of ITAC Working Groups and subcommittees

Coordinate funding and technical assistance to support the activities of all ITAC Working Groups and Subcommittees

Institute regularly scheduled coordination meetings with the ITAC Chair and the Chairs of all Working Groups and Subcommittees established by the ITAC

Establish and obtain funding and technical assistance to support an ITAC communications facility, newsletter and presence on the Internet

Establish and maintain a program to identify, monitor and report upon Fast Track projects



Encourage and facilitate interagency program manager organizations for the coordination and the distribution of information

Conduct such data gathering and inquiries as assigned by the ITAC

Secure and manage contract support as needed.

#### **3.6.1.4 JUSTIS System Manager**

The purpose of the position is to provide, leadership, management, supervision and direction to IT personnel of the DC Integrated Justice Information System (JUSTIS) staff. This position is responsible for the successful day-to-day operation of JUSTIS, the maintenance of JUSTIS, the in-house design and implementation of JUSTIS functionality, customer relations and training of JUSTIS users, and supervision of JUSTIS contractors.

##### **Goals:**

Communicating the goals and objectives of the ITAC to the JUSTIS organization

Managing systems upgrades and implementation

Managing system quality

Managing system performance

Communicating system events and status to the ITAC

Continued monitoring of legislative actions that could affect the deployed JUSTIS system or allow for increased information sharing opportunities

Continued monitoring of opportunities for increased system functionality

Maintaining liaison between all JUSTIS agencies

#### **3.6.1.5 Information Technology Security Officer (ITSO)**

In order to enforce security and carry the next critical projects forward, a key organizational stakeholder needs to be identified as the Information Technology Security Officer (ITSO).

The Security Office promulgates security policy planning and documentation requirements and conducts the following activities:

- The Security Office performs security audits
- The Security Office performs a security policy audits
- The Security Office reviews and enhances security infrastructure elements

### **3.6.1.6 Operations Department**

JUSTIS requires a well-trained operations staff for ongoing operations and administration of the system. Operations staff is critical to maintaining the functionality of the system by:

- Maintaining facilities personnel on a 24 by 7 basis.
- Maintaining disaster avoidance practices such as routine backups and preventive maintenance.
- Maintaining disaster recovery practices such as the development and exercise of a JUSTIS disaster recovery plan.
- Monitoring system use and maintaining log files.
- Monitoring system performance.
- Managing hardware and software licenses and maintenance contracts.

### **3.6.1.7 Help Desk Department**

In order to take advantage of all the JUSTIS capabilities, it is recommended that users once granted access, attend training. Also, once the user community becomes sufficiently large, as determined by the ITAC, a help desk will be needed to provide end-user support.

### **3.6.1.8 Applications Development Department**

The applications development department will be comparatively large during phased JUSTIS implementation and will reduce in number as the system nears full implementation. A single individual might fulfill a number of roles within this organization. These roles and their duties include:

**Web Site Content Originator**

The Content Originator creates content and maintains a fresh, valuable, quality electronic information product.

**Web Site Content Owner**

The Content Owners serve as the experts in a given content area. They have the responsibility of managing and providing updated information for a particular section of the site. The Content Owner is often the Content Originator but should always have review and approval authority.

**Web Site Content Authority**

The Content Authority approves and prioritizes content change requests. The Content Authority is an essential big picture gatekeeper role in the process and is the one most often overlooked.

**Web Site Enterprise Authority**

The JUSTIS Manager is the primary Enterprise Authority for JUSTIS. The JUSTIS Manager must approve all Internet content and Web sites.

**Implementation Manager**

The Implementation Manager assigns technical resources for changes to the Web site. After content is created and approved, the implementation process begins. Depending on the type of content and the work level of the technical team, different people with different skill sets may be required.

**Implementer**

Implementers prepare content for installation. Implementers include HTML programmers, graphics designers, scriptwriters, and any other technically skilled individuals required to prepare content for installation on the site. They will coordinate with the Content Authority to ensure the original intent is translated accurately to the site.

**Web Publisher**

The Web Publisher operates and manages the Web hosts.

**Web Application Developer**

Web Application Developers create, test, debug and maintain Web programs, Java Servlets, Java Server Pages, Active Server Pages and COM Objects.

**Database Developer**

The database developer works with agency legacy applications database administrators to understand, document and connect to participating agency databases.

### **3.6.1.9 Applications Maintenance Department**

The applications maintenance department will be comparatively small during phased JUSTIS implementation and will grow in number as the system nears full implementation. The roles and duties in this department are the same as in applications development.

### **3.6.1.10 Security Administration Department**

The security administrator is responsible for carrying out policies and procedures set forth by the Information Technology Security Officer. The Security Administrator:

- Maintains JUSTIS users by creating, deleting or modifying user accounts and access privileges.
- Liaises with security officers and administrators from JUSTIS agency participants.
- Assists with auditing and monitoring activities.
- Maintains security log file information.

### **3.6.1.11 Applications Maintenance Department**

The applications maintenance department will be comparatively small during phased JUSTIS implementation and will grow in number as the system nears full implementation. The roles and duties in this department are the same as in applications development.

### **3.6.1.12 Security Administration Department**

The security administrator is responsible for carrying out policies and procedures set forth by the Information Technology Security Officer. The Security Administrator:

Maintains JUSTIS users by creating, deleting or modifying user accounts and access privileges.

## JUSTIS BLUEPRINT

---

Liaises with security officers and administrators from JUSTIS agency participants.

Assists with auditing and monitoring activities.

Maintains security log file information.

## 4. Current Systems Summary

In order to implement JUSTIS with the functionality described in the previous section “Future JUSTIS User Community and System,” it is necessary to recognize the Information Technology (IT) challenges may exist by developing a summary of the current systems operating within the justice agencies. Each participating JUSTIS agency has developed a unique internal systems infrastructure, which presents challenges and opportunities to the implementation of JUSTIS. In each phase of JUSTIS (Proof of Concept, Phase 2, and Phase 3), agency systems were evaluated and documented to include the latest functionality, equipment, and impact on business processes.

Development of the Proof of Concept (POC) began with a thorough analysis of the current agency IT environments. During the POC, the JUSTIS implementation team developed a summary of the current agency IT environments by utilizing documentation and conducting interviews with ITAC members and selected justice agency personnel.

The ITLO provided the JUSTIS implementation team with documentation that represented proof-of-concept engagement requirements, administrative and technical infrastructure summaries and analyses of justice agency business processes and future plans. The table below highlights some of the important documentation provided.

Summary of CJCC provided documentation

Title	Description
Governance and Structure	Information about hierarchy of different work groups, their purpose and mission
CJCC ITAC	Contains information about Justice Agency Infrastructure Vision
Tracking Number Discussion	Tracking number importance and information about it
CJCC	Interagency Agreement on Information Technology
Comparisons of Definitions in Title 28 & found in State Laws	Table of Comparisons
Interagency automated Data	A CD containing information about different agencies information systems
Tracking Number Utilization	Information about Tracking Number Utilization

Interviews were conducted in an effort to gain further detail of current interagency business processes, specific agency IT environment, and each stakeholder’s JUSTIS

“vision.” All ITAC members and selected agency representatives were interviewed to get the most accurate depiction of each agency’s current systems.

At this time the JUSTIS implementation team also attended various ITAC work group meetings, namely the Technical Working Group and the Privacy & Security Working Group.

In Phase 2, the Justice Research and Statistics Association (JRSA) developed an Automated Reference Materials (ARM) database that was made available to all JUSTIS users via the secure JUSTIS website. The ARM Database provides a summary of all IT systems in each agency. Agencies are also able to update the information in the ARM database through the JUSTIS website as the status of their systems change.

Phase 3 introduced new functionality to the JUSTIS system including Core Data Transfer, Data Quality Alliance, and a Public Access website. These new functionalities evolved from further in depth research of agency systems and a series of Joint Application Development (JAD) sessions. The JAD sessions were conducted with agency representatives and members of the implementation team to define requirements for Phase 3 functionality. Through these processes, the knowledgebase of agency systems was more thoroughly defined.

The details of agency system infrastructure that are presented here have evolved through each phase of JUSTIS. This information will help in identifying the concerns and constraints for those who use, administer and manage these environments. The identification of the concerns and constraints are critical to the development of the roadmap that will define the steps necessary to achieve the future JUSTIS system. This section provides a high-level summary of the known current IT environment that was in place within each of the criminal justice agencies at the completion of the POC<sup>4</sup>. The following sections focus on three primary areas:

- Security Infrastructure
- Network Infrastructure
- JUSTIS Agency Legacy Applications and Data

## 4.1 Security Infrastructure

A required functionality of JUSTIS is to allow access to criminal justice data. Accessing criminal justice data through a technical architecture such as that utilized by JUSTIS requires an emphasis on security. This emphasis is addressed in JUSTIS

---

<sup>4</sup> At the time this version of the Blueprint was created, the agency systems information provided represents the latest data available in the ARM database and from the knowledgebase of the implementation team. However, this data may not be accurate in some cases where the agency has not updated the ARM database, or the implementation team is unaware of recent system updates.

deliverable number 1.1.2, JUSTIS Security Architecture. This deliverable describes the current JUSTIS security architecture deployed in JUSTIS Phase 3.



The uniqueness of the relationship of justice agencies of the District of Columbia has lead to a complex web of interconnectivity as exemplified below<sup>5</sup>. District of Columbia agencies are centered on the DC Wide Area Network (DC WAN), while Federal justice agencies have independent WANs. Although the Federal Agencies each have independent WANs, they many also have connections to the DC WAN.

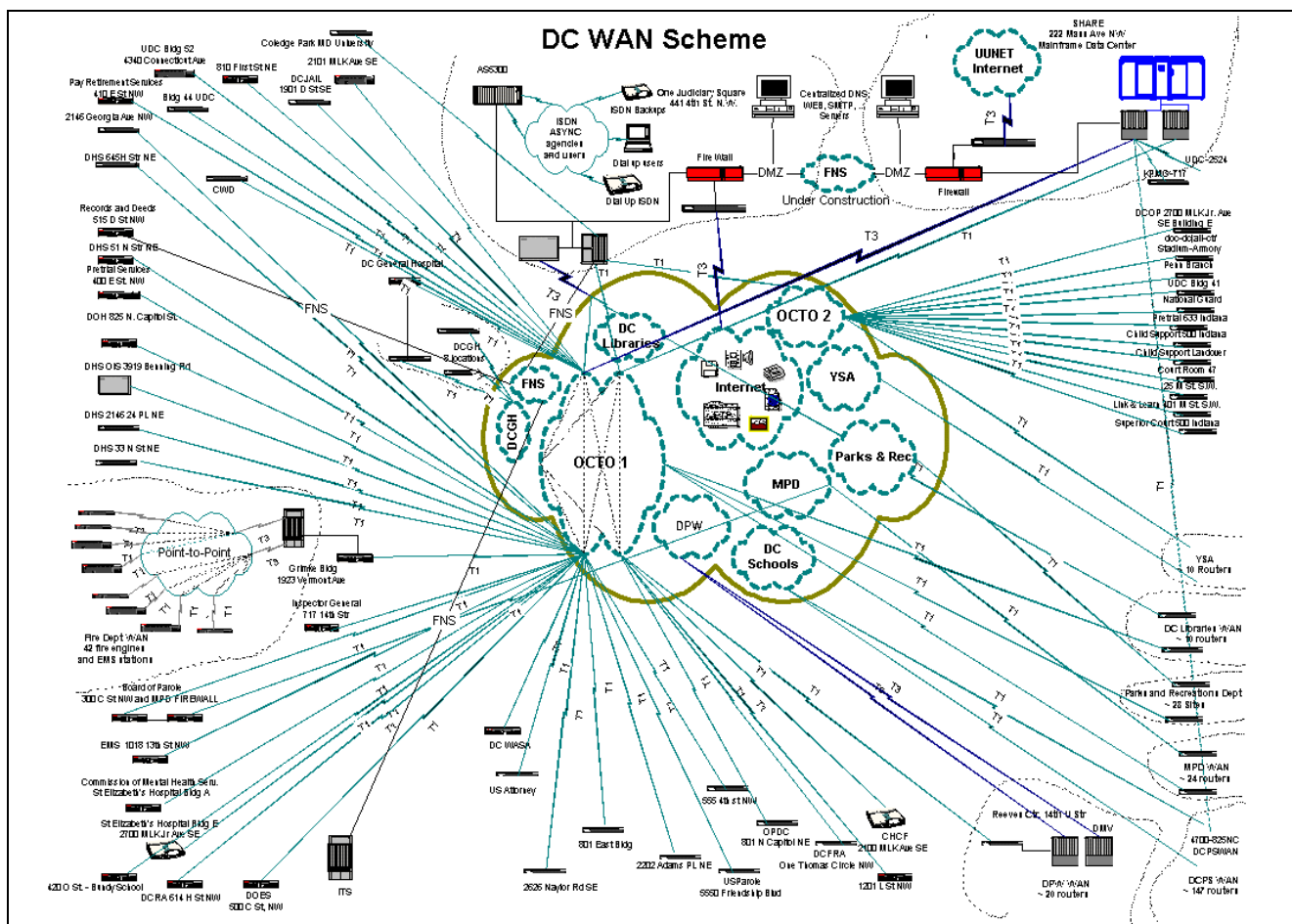


Figure 22 – Justice Agency Connection Points

<sup>5</sup> This diagram derived from the DC WAN diagrams provided by OCTO (circa October 2002).

# JUSTIS BLUEPRINT

## JUSTIS Agency Network Summary (October 2002)

Agency	DC WAN Connectivity	Network Topology	Network Hardware	Operating System	Protocols	WAN Services	Service Provider	Network Security	Maintenance
Office of the Chief Tech. Officer	T1 1 Site S Clouds, 464 Sites	Ethernet 10 Base – T Fast Ethernet	Cisco kentrox Digital Line	Novell NetWare 3.12-4.1 3 Servers MS NT Server 4.0 18 Server	TCP/IP IPX/SPX	9.6, 56K, T2, T3 ISDN	Bell Atlantic, UUNET	Cisco Pix 4.25	Internally Managed
Office of Corporation Counsel	T1 1 Site	Ethernet 10Base – T	Cisco Compaq	MS NT Server 4.0 10 Servers	TCP/IP Telnet	N/A	Bell Atlantic	MS Firewall Proxy 2.0	Internally Managed
CSOSA	T1 1 Site	Ethernet Fast Ethernet	Cisco	Novell NetWare 5.0 7 servers MS NT Server 4.0 20 Servers	TCP/IP IPX/SPX	Bell Atlantic Point to Point T1 fiber	UUNET	Secure Firewall Borderware	Internally Managed
DC Dept. of Correction	T1 25 Site	Ethernet Fast Ethernet	Cisco	20 Novell NetWare 4. 1 servers MS NT Server 4.0 5 Servers	TCP/IP IPX/SPX	Bell Atlantic T1	Bell Atlantic	Novell Firewall Border Messenger 3.0	Outsourced
DC Superior Court	T1 1 Site	Ethernet 10Base –T Fast Ethernet	Cisco Compaq Dell	Novell NetWare 4.0 1 Server MS NT Server 4.0 16 Server	TCP/IP IPX/SPX NetBEUI	Bell Atlantic T3	World Com MCI UUNET	Borderware	Internally Managed
Metropolitan Police Department	T1 25 Sites	Ethernet Fast Ethernet 10Base –T Gigabit Token Ring	Cisco 3Com	Novell NetWare 5.0 38 Servers MS NT Server 4.0 7 Servers Unix 6 servers	TCP/IP IPX/SPX	Bell Atlantic T1 9.6 56K	Digex	Checkpoint Firewall 4.0	Internally Managed
Public Defender	T1	Ethernet 10/100	Cisco	Windows NT Server 4.0	TCP/IP	Bell Atlantic T1 – 3	UUNET	MS Proxy 2.0	Internally Managed
US Attorney		Ethernet	Cisco	NT 4.0 Unix Servers	TCP/IP Telnet	Sprint ATM	Sprint	Raptor Firewall	Internally and Outsourced
US Parole Commission	T1		Cisco						

Agency	DC WAN Connectivity	Network Topology	Network Hardware	Operating System	Protocols	WAN Services	Service Provider	Network Security	Maintenance
Youth Services Administration		TCP/IP	Cisco	MS NT Server 4.0 9 Servers		Bell Atlantic T1 and 56 K		Cisco Firewalls	

### 4.3 JUSTIS Legacy Systems

Legacy information systems provide the first tier of the JUSTIS application. These systems contain the data that is virtually integrated by all of the JUSTIS applications. Below is a list of the legacy information systems currently accessed by JUSTIS. Additional details regarding these and other CJCC legacy system can be found in the Automated Reference Materials database, developed by the ITAC, and in the Phase 2 version of the JUSTIS Blueprint, dated September 24, 2001.

JUSTIS Agency Legacy Application Summary

Agency	System Name	Description
Court Services & Offender Supervision	OASIS – Offenders Automated Supervision Information System	Case management system used by CSO's (Community Supervision Officers) to track the status of parolees and probationers released to CSOSA.
District of Columbia Child and Family Services Agency	FACES -	
District of Columbia Department of Corrections	JAACS – Jail and Community Corrections System	New system includes CRISYS and JALAN functionality along with cautions / alerts / separations, automated clearances, inmate pay, compliance support, staff scheduling / training / certification, intelligence / investigation / incident tracking, medical screening, food management, mug shots, fingerprints, document imaging, enhanced case management, objective classification, inmate property management, work/community supervision, program

Agency	System Name	Description
		participation, and bar code identification..
District of Columbia Metropolitan Police Department	Washington Area Law Enforcement System (WALES)	State files & interface for NCIC, warrants, MPD registration files, copy of DMV permits and registrations, NCIC communications for external agencies, other agencies software (ABA DABA, CRISYS).
	Criminal Justice Information System (CJIS)	Criminal history information (MPD booking, Superior Court dispositions, DCDOC prisoner status, parolee status), Statistical information, and reports.
District of Columbia Department of Motor Vehicles	Destiny	DB2 information system that maintains all registered vehicle and driver information for the District of Columbia.
Office of Corporation Counsel	ProLaw	Attorney case management system, developed on Microsoft SQL Server Database platform.
Public Defender Services	Microsoft Exchange Sever	PDS currently contributes attorney contact information only. This information is contributed directly from the agency's Microsoft Exchange Server.
PreTrial Services Agency	PRISM	Defendant tracking database, built on Microsoft SQL Server. This database contains both defendant pretrial data and drug testing information.
District of Columbia Superior Court	Criminal Information System (CIS)	Criminal Record maintenance system that contains felony, misdemeanor, and major moving file from 1978-1998. IDMS/R Cobol.
	Juvenile Information System (JISRA)	1981-2002 Juvenile records with retrieval by case#, docket#, social file#, soundex file#. Is a flat/VSAM data file.
United States Attorney's Office	Replicated Criminal Information System (RCIS)	Imports CJIS, CIS data on daily basis into Oracle database. Tracks arrests, court cases, witnesses, and USAO specific data. Generates calendars, caseload, defendant history, statistical, and other management reports.

Agency	System Name	Description
U.S. Parole Commission	Decision Recording And Monitoring system (DRAM)	The system is used to record and monitor individual paroling decisions. When a user is about to
	Document Automation System (DAS)	This system is used to prepare standard prisoner documents. The system uses Microsoft's Visual Basic for Applications to produce Word documents. Address information and prisoner names are inserted from standard databases. The system also prompts users to select standard text inserts. Documents created by the system can, at the users' discretion, be submitted to be automated overnight faxing system. Also, all documents created by the system are included in the DOCVU system and selected data elements are written to the DRAM system.
United States Probation Office	PACTS – Probation Automated Case Tracking System	This is the automated case tracking system used by USPO. This information system has yet to be integrated into the JUSTIS infrastructure.
Department of Human Services' Youth Services Administration	Juvenile Information Management System (JIMS)	Tracks juvenile cases and maintains client records of basic personal and family information and history, as well as the tracking of client movements through different placements during an YSA stay.

## 4.4 Current Network Design

The following diagram displays the current JUSTIS network layout developed during JUSTIS Phase 3. The diagram illustrates JUSTIS server placement and the current replicated data locations. The diagram will be continually updated to depict all new developments, as JUSTIS is continually deployed.

# JUSTIS BLUEPRINT

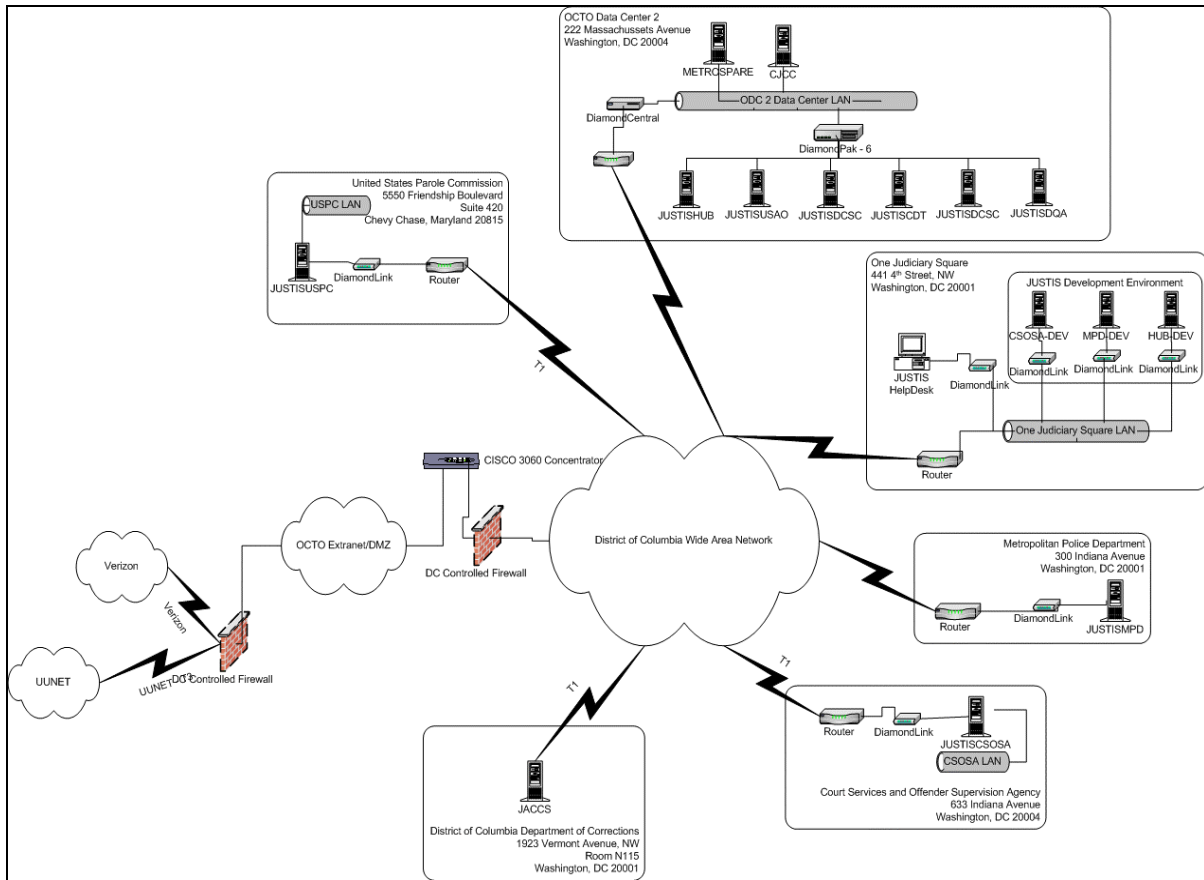


Figure 23 – JUSTIS Phase 3 Technical Architecture

The following diagram uses the same architecture relationships as Figure 23, but shows the key JUSTIS operational databases that are found on each server.

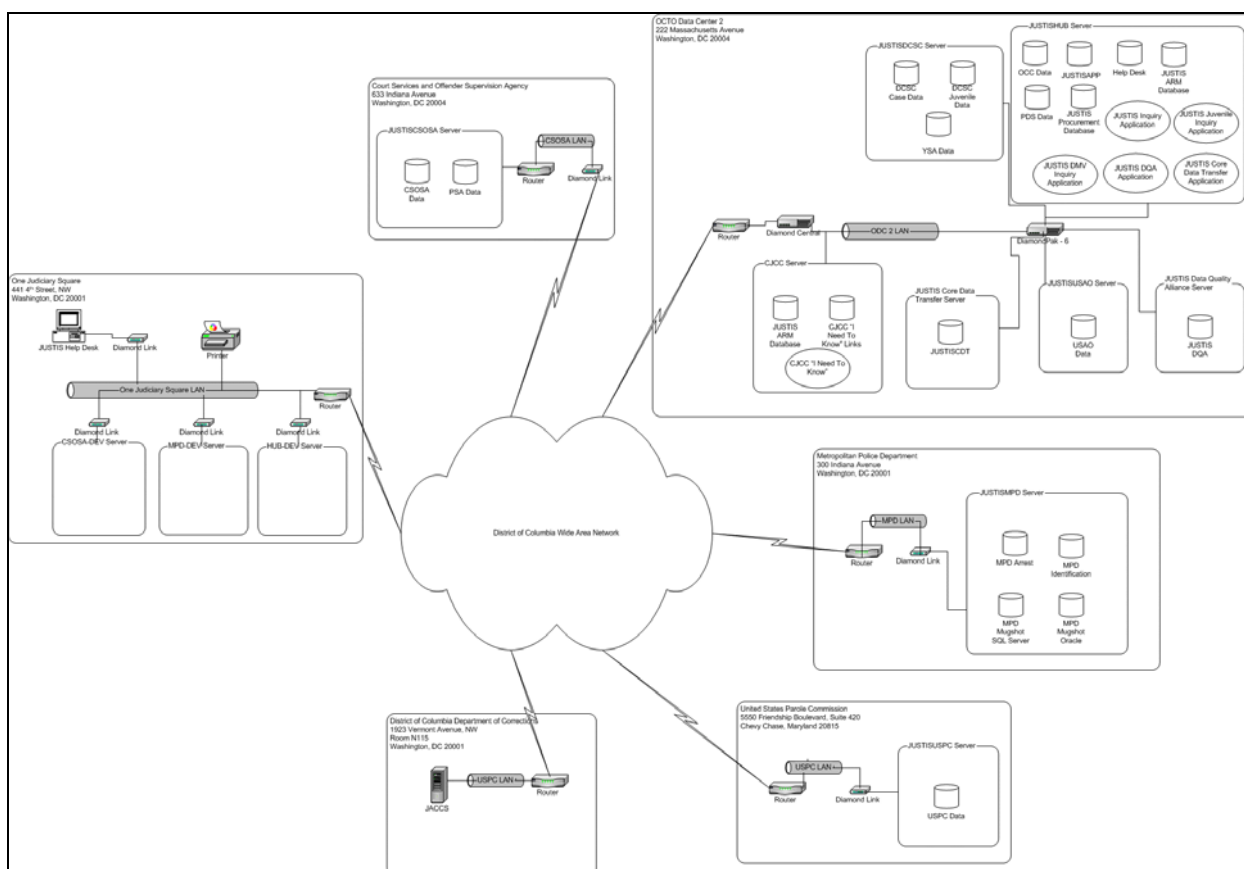


Figure 24 - JUSTIS Phase 3 Database Diagram

## 4.5 User Workstations

Deployment of an application such as JUSTIS across fourteen different agencies that internally are at various stages of information technology sophistication can produce an application that requires a large amount of maintenance. Recognizing this potential difficulty, the ITAC required that JUSTIS application be developed utilizing the contemporary technologies of the Internet. JUSTIS has leveraged the wide use of Internet technologies in its development. This has led to the development of an application that has taken advantage of open web components in its architecture. The result is an application that is browser based and therefore easily deployed to the users' workstation and requires minimal maintenance in its deployment.

The minimal JUSTIS user workstation requirements are as follows:

**Browsers** – Internet Explorer 4.0 or higher or Netscape Navigator 4.0 or higher. JUSTIS works most effectively with Internet Explorer.

**Computer Processor** - 486DX/66 MHz or higher processor.

**Operating System** – Windows ME, Windows 95, Windows 98, Windows 2000, Windows NT 4.0, or Windows XP.

**Memory** - For Windows 95, Windows 98, and Windows 2000: 16 MB (megabytes) of RAM minimum. For Windows NT and XP: 32 MB of RAM minimum.

JUSTIS is a secure Intranet. This requires security components in a browser that may not be included in the version currently residing on the users' workstation. The users' browser must have cipher strength of 128-bit. Steps to view and modify the users' browser cipher strength in both Microsoft's Internet Explorer and Netscape Navigator are detailed in the JUSTIS Phase 3 User's Manual.

Through the end of Phase 3, fourteen user agencies have taken advantage of the ease of deploying a browser based application with minimal to no modification of their current workstations. This is the basis for the conclusion that all user agencies either meet or exceed the minimal user workstation requirements detailed above.

## 4.6 JUSTIS POC

This section discusses the infrastructure and operations that were in place at the conclusion of the POC on January 18, 2001. As stated in previous sections, the POC involved three agencies, MPDC, PSA, and CSOSA. The central objective of the delivery of the POC was to provide the CJCC member agencies with a model of data sharing functionality, while adhering to the council's business requirements.

### 4.6.1 *Proof of Concept Infrastructure*

The following diagram illustrates the network infrastructure that resulted from the implementation of the POC. The POC involved the installation of three primary servers and the creation of a Development Environment. Further details concerning the primary server configuration and location are included JUSTIS deliverable number 1.14, JUSTIS Hardware Expansion Plan.



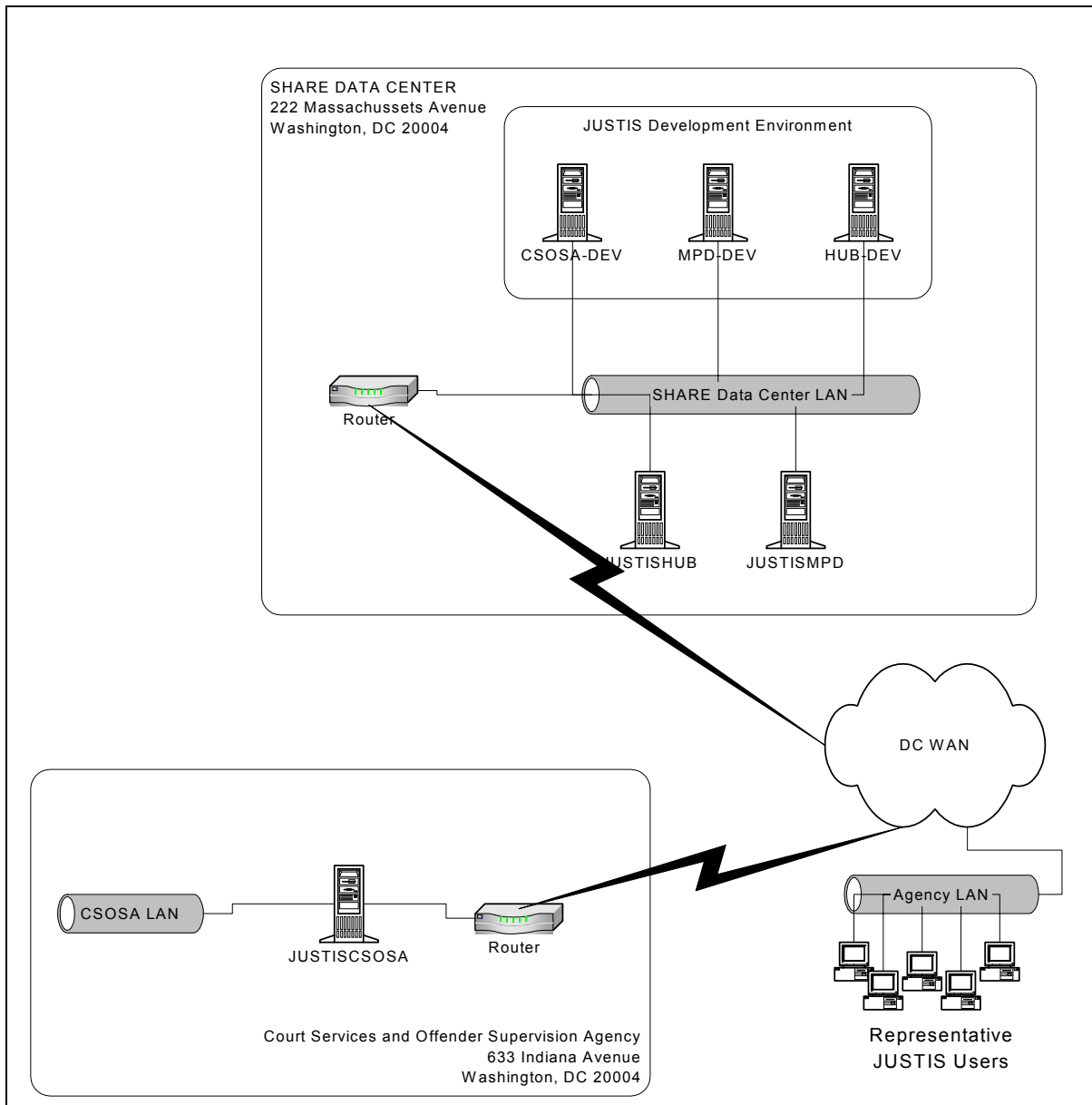


Figure 25 – JUSTIS POC Network Diagram

#### 4.6.2 POC Operations

The POC data sharing functionality is enabled through three primary servers, JUSTISHUB, JUSTISMPD, and JUSTISCSOSA. The JUSTISHUB is the central facility, containing the JUSTIS applications and web interfaces. The two

secondary servers contain the agency specific data. The JUSTISMPPD server maintains the corresponding MPDC database, while the JUSTISCSOSA server maintains the databases for both CSOSA and PSA.

Data sharing functionality is established through the use of the JUSTIS Inquiry Application, located on the JUSTIS Hub server. This application has been developed as a broker between the user inquiry and the agency data. Based upon user inquiry, the application returns to the user what records are available and which particular agency has the records. The user then is able to select records for review. The inquiry application is able to retrieve the record from the particular agency and return the encrypted record to the user via the DC WAN. Please refer to the Future System section for a more detailed explanation of the data sharing functionality.

#### 4.6.3 *POC Accomplishments*

The expectations for the POC were limited in scope but huge in impact. The POC could be summarized as: Design, Develop & Deploy Web Browser solution demonstrating the ability of Multiple Agencies to share information. The POC accomplished exactly that. The larger impact was that it proved that this concept was realistic, was workable and fit the diverse DC justice community. This engagement involved the entire justice community and won the unanimous support of all ITAC agencies. The completion of the POC allowed the CJCC to make an informed “go / no-go” decision about the future of JUSTIS. The presentation to the CJCC was successful and Phase 2 was allowed to proceed.

The POC was designed and implemented within the Blueprint's concept of an integrated, citywide integrated justice information system. This system utilized open Internet technologies and standards to access information from diverse justice agency systems. This approach used an Intranet dedicated for use only by justice agencies under a common Web browser interface. The POC was successfully completed on schedule, and within budget, in December 2000.

### 4.7 JUSTIS Phase 2

This section describes the expanded JUSTIS infrastructure as it was at the end of Phase 2 on September 30, 2001. This infrastructure built upon the existing POC infrastructure by adding servers to support the data contribution expansion as outlined in the Phase 2 statement of work.

#### 4.7.1 *Phase 2 Infrastructure*

JUSTIS Phase 2 Infrastructure maintains the same conceptual framework deployed in the POC. The JUSTISHUB server remains the central facility to which all agency servers connect. The primary difference between the POC and Phase 2 infrastructure is the addition of the JUSTISUSAO, JUSTISUSPC, JUSTISDCSC and JUSTISBackup servers. The implementation of data encryption devices between the agency servers and the JUSTISHUB was initiated in Phase 2. Also incorporated with the implementation of Phase 2 is the direct Internet connection to the Jail and Community Corrections System (JACCS) maintained by the District of Columbia Department of Corrections (DOC).

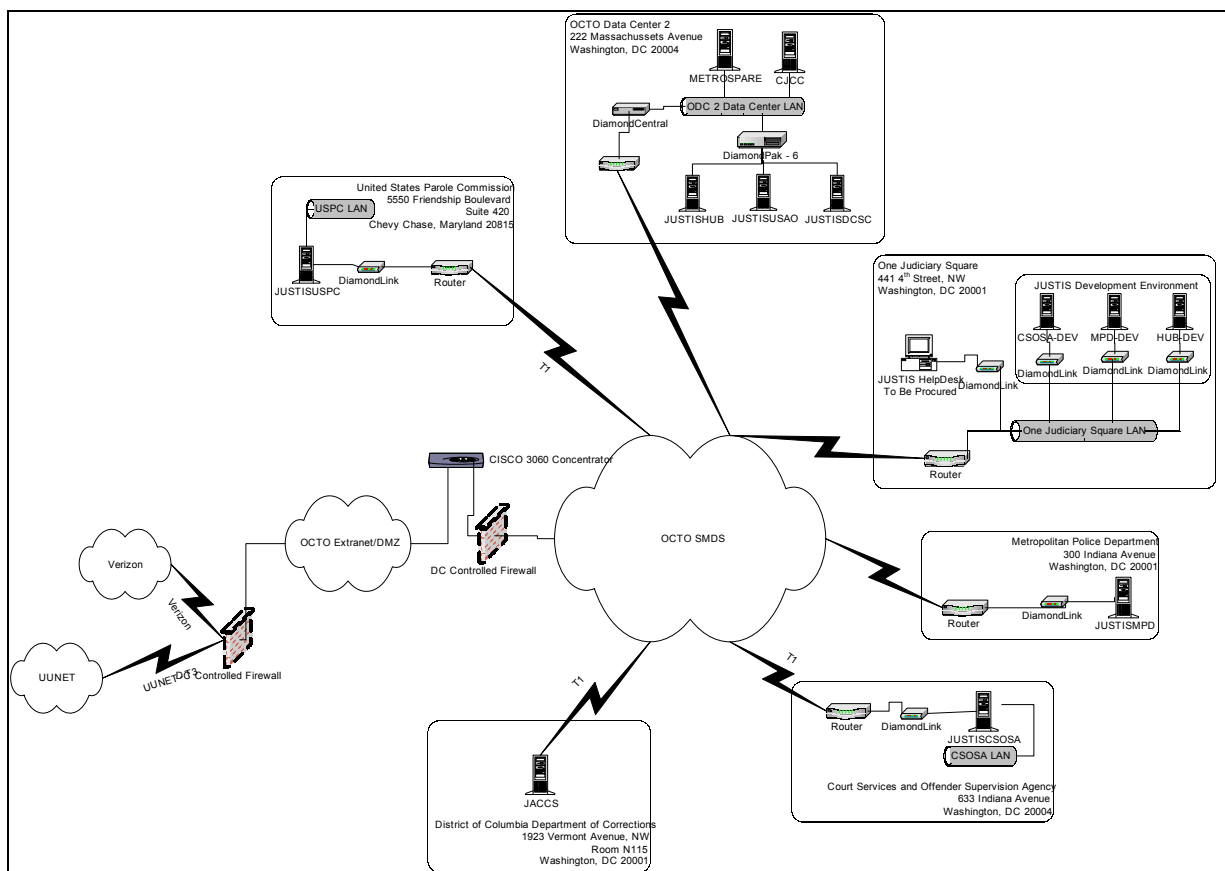


Figure 26 - JUSTIS Phase 2 Architecture

#### 4.7.2 Phase 2 Operations

Although significant hardware expansion is incorporated with the implementation of Phase 2, the operation of JUSTIS remains the same. **Figure 24** illustrates the where the replicated data is stored. The JUSTISHUB will access the additional databases located on the servers and continue to provide a unified view to the JUSTIS users.

#### 4.7.3 PHASE 2 Accomplishments

The expectations for Phase 2 were significant. With the JUSTIS concept having been proven in the POC, Phase 2 was expected to:

- Implement a full production, operational environment
- Provide best practice security, meeting or exceeding all participating systems' security
- Expand the JUSTIS system to include access by personnel in every ITAC member agency
- Increase data contributions from every ITAC agency's legacy system.

Each of these expectations was fully met. The functionality offered by JUSTIS during the POC, while significant, did not begin to exploit the potential for this system. Concepts and requirements for additional functionality were drawn from a number of sources including input from interviews and analysis involving ITAC members and their technical staff. Additional input was the product of prior experiences of the POC city/contractor team, accomplishments by other states, and the vision of the CJCC and staff. A number of additional functions were identified for JUSTIS, reviewed by the ITAC, and documented for development in the JUSTIS Blueprint.

The results of JUSTIS Phase 2 can be succinctly summarized as:

- Full Operation – JUSTIS went from a demonstration environment to a fully operational system with developments staff, operations staff and a fully staffed JUSTIS help desk
- Total Contribution – JUSTIS grew from three users contributing data from their legacy systems, to every participating ITAC agency allowing data from their legacy system being managed and shared through JUSTIS
- Universal Access – JUSTIS grew from limited access from only the major agencies contributing data during the POC to a system managing and allowing access from any requesting person in any participating ITAC agency, within the constraints of a fully operational access control methodology.

The benefits provided by the end of Phase 2 included: providing users with timely information on offender status, providing a unified view – a user in one agency can see all agencies contributed data, enabling secure collaboration among authorized users, increased speed in processing cases, improved quality of public safety decisions, providing the architecture to support future functionality.

## 4.8 JUSTIS Phase 3

### 4.8.1 *Phase 3 Infrastructure*

JUSTIS Phase 3 Infrastructure built upon the Phase 2 design. The final architecture for Phase 3 is depicted in Figure 23 – JUSTIS Phase 3 Technical Architecture. The JUSTISHUB server remains the central facility to which all agency servers connect. However, two additional servers were added to carry out the functions of Core Data Transfer (CDT) and Data Quality Alliance (DQA). Phase 3 also included a Public Access website, the integration of DMV license data, and DCSC juvenile data, however, these additions did not affect JUSTIS infrastructure.

### 4.8.2 *Phase 3 Operations*

Phase 3 did not alter the operations established in the POC or Phase 2. JUSTISHUB remains central to each agency's data contribution for the Inquiry Application. However, new hardware and operations were added as part of CDT and DQA. In addition, the integration of DMV license data and DCSC juvenile data required the establishment of a data contribution design for each data set.

CDT involves the regular transfer of a uniform set of data to all agencies in various formats so that agencies will have easy access to critical data. The core data set is transferred to the CDT server and then distributed to JUSTIS agency servers where each agency can access the data. The details surrounding this process can be found in the Core Data Transfer Design Document.

DQA offers the JUSTIS community an opportunity to recognize, record, and resolve criminal justice data errors and inconsistencies. A DQA server was added to record and index all data errors recognized by the JUSTIS community. The details of the DQA process are found in the Data Quality Alliance Design Document.

As with all other contributed data, DMV and DCSC juvenile data is transferred to the JUSTISHUB and displayed in HTML format on the JUSTIS website. The details of the DMV and DCSC juvenile data contribution are found in their own respective data contribution design documents.

### 4.8.3 *Phase 3 Accomplishments:*

Phase 3 concentrated on providing functionality beyond the basics of a fully operational system with universal access. Functionality requirements had to take into account reconsideration of priorities, greater expectations for improved data quality and offender record consolidation based upon the access provided by Phase 2. Phase 3 also increased potential for the use of the CJCC.DC.gov website, and new programmatic opportunities for the justice community.

Phase 3 activities were centered on, but not limited to:

- Data Quality
- Notification
- Core Data Transfer
- Public Access
- Strategic Planning for allied agency “families”
- DC Tracking Number Implementation

These goals were the primary thrust of the JUSTIS Phase 3 program. These accomplishments added basic services and routines never before provided to justice agencies within the District of Columbia. They represent not only the literal work products and accomplishments, but also the more intrinsic success of collaboration of all the primary justice agencies in the city: executive agencies at city and federal levels, judicial, and independent agencies.

The accomplishments of Phase 3 were numerous and varied. The listing below presents the more significant accomplishments:

- **Core Data Transfer (CDT)** – All agencies have all arrest data automatically delivered to their system. All agencies / users have listings of up to 15 days worth of arrest data in five different formats upon inquiry
- **Data Quality Alliance (DQA)** – All users have a fully automated tool to identify and report errors and inconsistencies to “owner” agencies. All owner agencies can examine reports, contact user, record actions. All activities are available in a permanent history with each record. The CJCC and the ITAC have access to Evaluation & Review Tool.
- **District of Columbia Public Safety Tracking Number Centrally Implemented (TRK)** – A single access number is available for all agency

records. Now, all portions of a criminal justice cycle can be tied together through JUSTIS.

- **DC Superior Court Juvenile Data Availability** – Agencies serving and protecting children now have greater access to data from which to make better-informed decisions.
- **DC DMV Availability** – JUSTIS users now have greater access to DMV data.
- **Public Access** – “I Want to Know” / “Yo Quiero Saber” – Tangible benefits to citizens from JUSTIS investment
  - Bilingual access
  - ADA standards met
- **Notification Specification** – The design of a notification system leveraging the existing JUSTIS infrastructure will provide the basis for interactive data. Interactive data will increase the opportunity for JUSTIS users to make informed decisions during the course of business.
- **Special Order** – Established and strengthened the foundation for sharing juvenile data among authorized agencies through use of JUSTIS
- **Juvenile Inquiry Tool** – JUSTIS offers the juvenile data community a more individualized inquiry method. The Juvenile Inquiry Tool provides a visual confirmation of application of security and access rules and recognition of laws.
- **Mug Shots** – As of Phase 3 JUSTIS integrated the arrest mug shot into the JUSTIS Inquiry Tool. Now MPD mug shots can be accessed by all authorized agencies.
- **Secure Internet Access** – Expansion to all authorized criminal justice agencies within the District of Columbia, whether or not they are directly connected to the DC WAN. This has been successfully demonstrated with access of JUSTIS by the U.S. Department of State – Diplomatic Security and the U.S. Probation Office
- **Integration of Child and Family Services Agency and the U.S. Probation Office** – JUSTIS Phase 3 concluded with the integration of the District of Columbia Child and Family Services Agency and the U.S. Probation Office.

As seen in this section’s discussion, the District of Columbia integrated justice information system, JUSTIS, has been developed through a series of



manageable steps, the last of which, Phase 3, was completed this month. The development of JUSTIS continues to be managed and controlled by the Information Technology Advisory Committee (ITAC), a CJCC standing committee serving as the JUSTIS “Board of Directors.” The ITAC hired an Information Technology Liaison Officer (ITLO) to serve as the motivator, facilitator, and manager of system development.

The ITAC and the ITLO documented a vision for an information system for the justice community in the District of Columbia on the POC Blueprint. That JUSTIS Blueprint identified a model that met the vision’s goals and objectives. The ITAC has moved in just two years beyond that vision, beyond the planning mode, to the development and implementation of an integrated justice information system with the following participating agencies both accessing and contributing data for the benefit of a justice community that now includes:

- Superior Court of the District of Columbia
- Office of Corporation Counsel
- Metropolitan Police Department
- Pretrial Services Agency
- Court Services and Offender Supervision Agency
- District of Columbia Department of Corrections
- Office of the United States Attorney for the District of Columbia
- Public Defender Service
- United States Parole Commission
- Department of Human Services’ Youth Services Administration
- DC Department of Motor Vehicles
- Child and Family Services Agency
- United States Probation Office

Access by allied justice agencies within the District has been approved by the ITAC and will be actively pursued as this latest phase of development ends. The newest non-ITAC JUSTIS user is the U.S. Department of State. Thirty-two additional DC law enforcement agencies will be invited to share those portions of JUSTIS data authorized by the data contribution agencies. Interest in access has been expressed by both Maryland and Virginia judicial and executive department agencies.

The JUSTIS facility is supporting the sharing of data in ways never before possible with agencies that never before could access, much less find, critical offender data. The goal of JUSTIS is to provide timely, accurate and complete data that allows justice officials to make better-informed decisions.

## 4.9 Summary

The information presented above provides a summary of the current IT environments within the justice agencies, and a brief description of the JUSTIS network environment that resulted from the implementation of the POC, JUSTIS Phase 2 and Phase 3. This information will be compared with the IT infrastructure requirements set forth in the Future Systems section of the JUSTIS Blueprint. This comparison generates a list of “gap” points that are laid out in the next section of the document. These “gap” points provide the basis for the development of the roadmap, which will present a logical process for a multi-phased implementation of JUSTIS.

It is worth noting that CJCC member agencies and OCTO are constantly working to enhance their information systems and the corresponding infrastructures. Therefore, the data presented here is only as accurate as the data available at time of publication. Moreover, the deployment of the ARM database will provide the facility that will shorten the lag time between agency information system improvement and CJCC recognition and documentation of the improvement. The ARM database will provide the developers of the Blueprint a resource that will support the Blueprint update effort. The support provided will ensure the data contained in this section will be relatively up-to-date.

## 5. Roadmap

### 5.1 Introduction

This Blueprint document began with a definition of the system's mission and business requirements. It then moved on to a description of the complete vision for the future JUSTIS system once it has been fully developed and implemented. Those sections collectively define the end-state goal for JUSTIS.

More specifically, section 3, titled Future JUSTIS User Community and System details the envisioned core functionality of JUSTIS.

- JUSTIS Data Inquiry Applications
- Searches
- Static Screens and Printed Reports
- Data Transfer
- Notification Services
- Threaded Discussion Groups

To date, JUSTIS has either fully accomplished or proven the feasibility of five of the six core functionalities. JUSTIS Data Inquiry Applications, Searches, Static Screens and Printed Reports, Data Transfer, and Threaded Discussions Groups are functionalities that are available through JUSTIS today. The remaining core functionality, Notification Services, is a future functionality that has been conceptually designed but as of yet not implemented and therefore still remains as a gap to full development.

This section presents an analysis of this and other gap areas between where we are at the end of Phase 3 (section 4, titled Current Systems Summary) and where we want to be (section 3, titled Future JUSTIS User Community and System). Once these gap areas are identified, organized and prioritized, a roadmap is presented. This roadmap shows a number of steps towards the full implementation. The following diagram depicts how we have proceeded through this document, and we are now in the final steps:

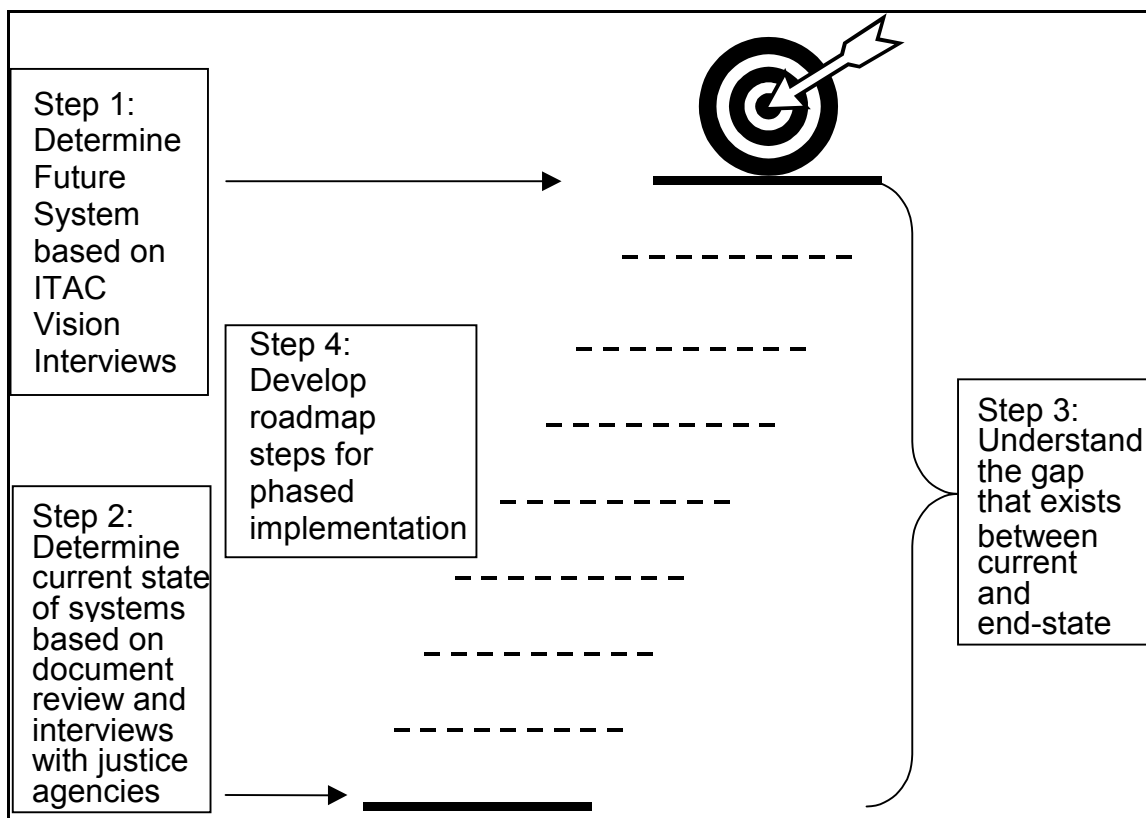


Figure 27 – Blueprint Format

JUSTIS has been and will continue to be implemented in phases. This allows the JUSTIS user community to realize short-term gains while proceeding toward the entire vision. Multi-phased implementation also allows the system to keep in time with contemporary technologies throughout the implementation. The roadmap defines the phased implementation.

## 5.2 Gap Areas Prioritized

The variance between current environment capabilities vis-à-vis the environment necessary to support the full JUSTIS system is analyzed in this section. Initially, JUSTIS was a completely new concept for the District of Columbia and the gaps were substantial. Over the past twenty-eight months, with the implementation of the POC, Phase 2, and Phase 3, the initial set of gaps have been significantly reduced.

However, the successful development of JUSTIS through Phase 3 allowed the JUSTIS community to recognize even greater potential for the system. While the initial vision for JUSTIS has been largely achieved, there remain outstanding goals,

and in addition, the vision itself continues to evolve to include new goals. The JUSTIS community recognizes several new areas for growth that will make JUSTIS a sustainable and effective tool. In order to make this dynamic JUSTIS vision a viable and workable objective, each goal is placed in a framework that classifies and prioritizes the goal based on two criteria - feasibility and the positive impact on the success of the system. The following table illustrates this framework by sorting each of the goals based on these criteria.

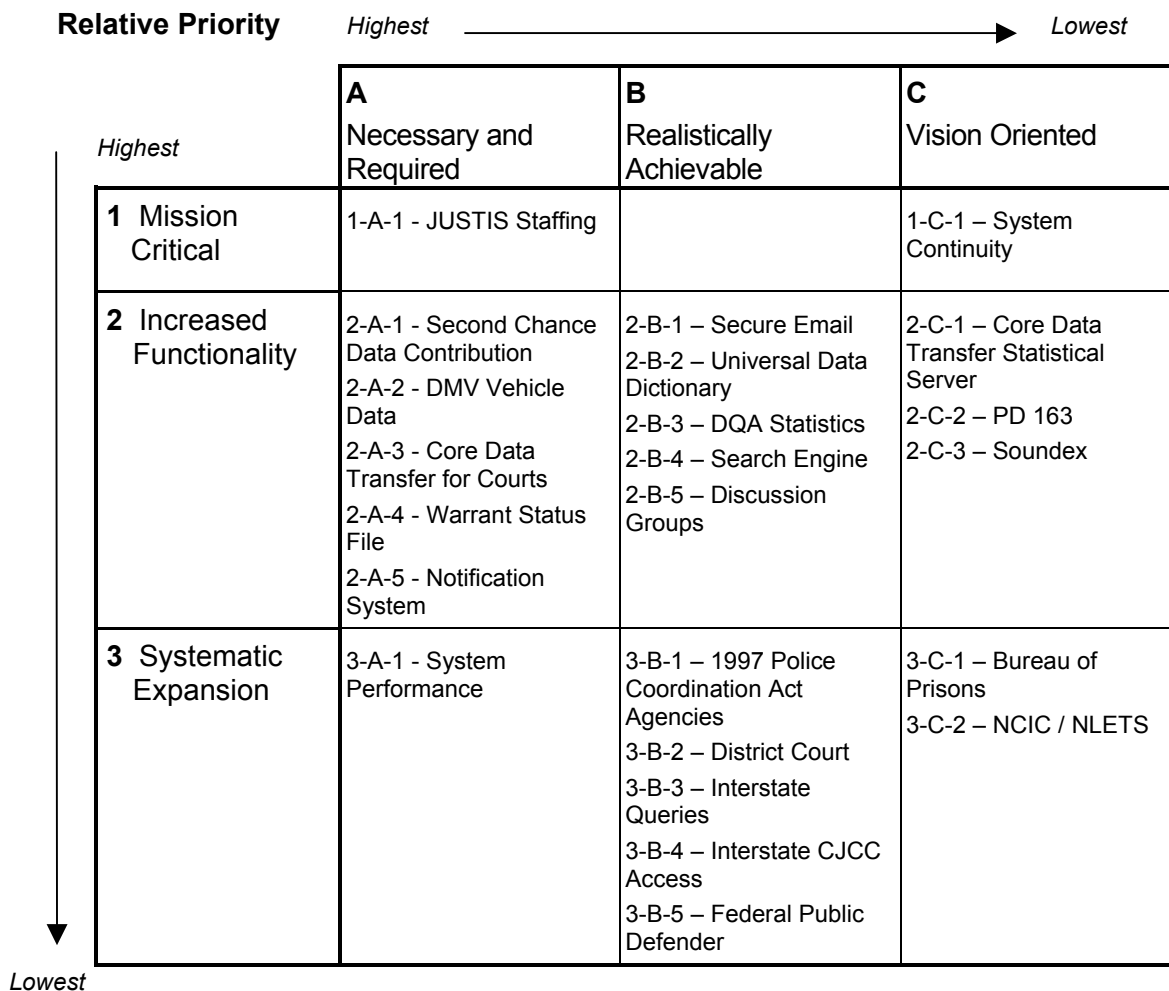


Figure 28 - JUSTIS Priority Matrix

## 5.2.1 Necessary and Required

### 5.2.1.1 Mission Critical

#### JUSTIS Staffing - 1-A-1

The implementation of the attached personnel organization chart is mandatory for the future operation of JUSTIS. The chart maintains the relationship between the JUSTIS system and the ITAC, while establishing

line responsibilities to administer, manage and maintain the system and its security.

The following organizational chart shows the immediate needs for JUSTIS staffing. Currently, at the end of Phase 3, only the ITAC, ITLO, and ITSO exist. Proper staffing for the other positions is a mission critical task that needs immediate attention.

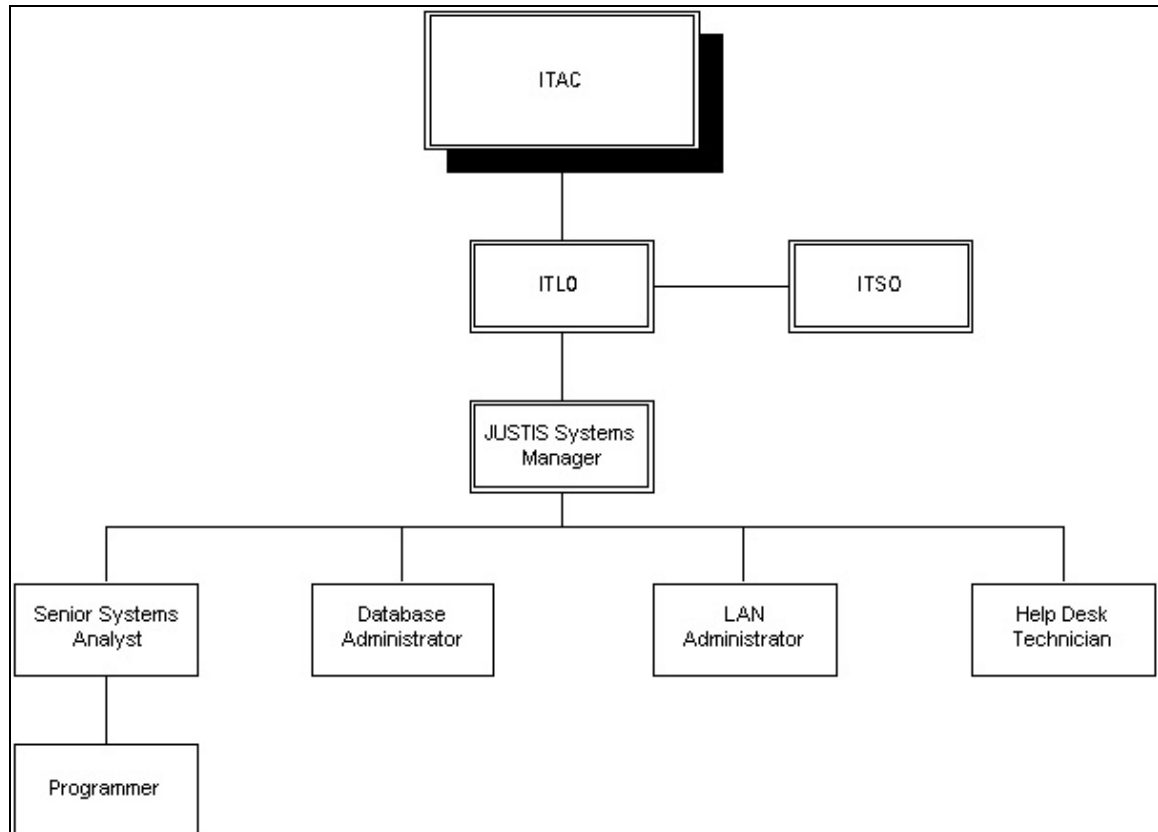


Figure 29 – Proposed JUSTIS Administrative and Management Structure for Current Support and Maintenance

As JUSTIS grows encompass a larger community and scope of functionality, the organizational structure will need to accommodate a larger workload to continue development, operation, and maintenance of the system. The future JUSTIS organizational structure is shown below.

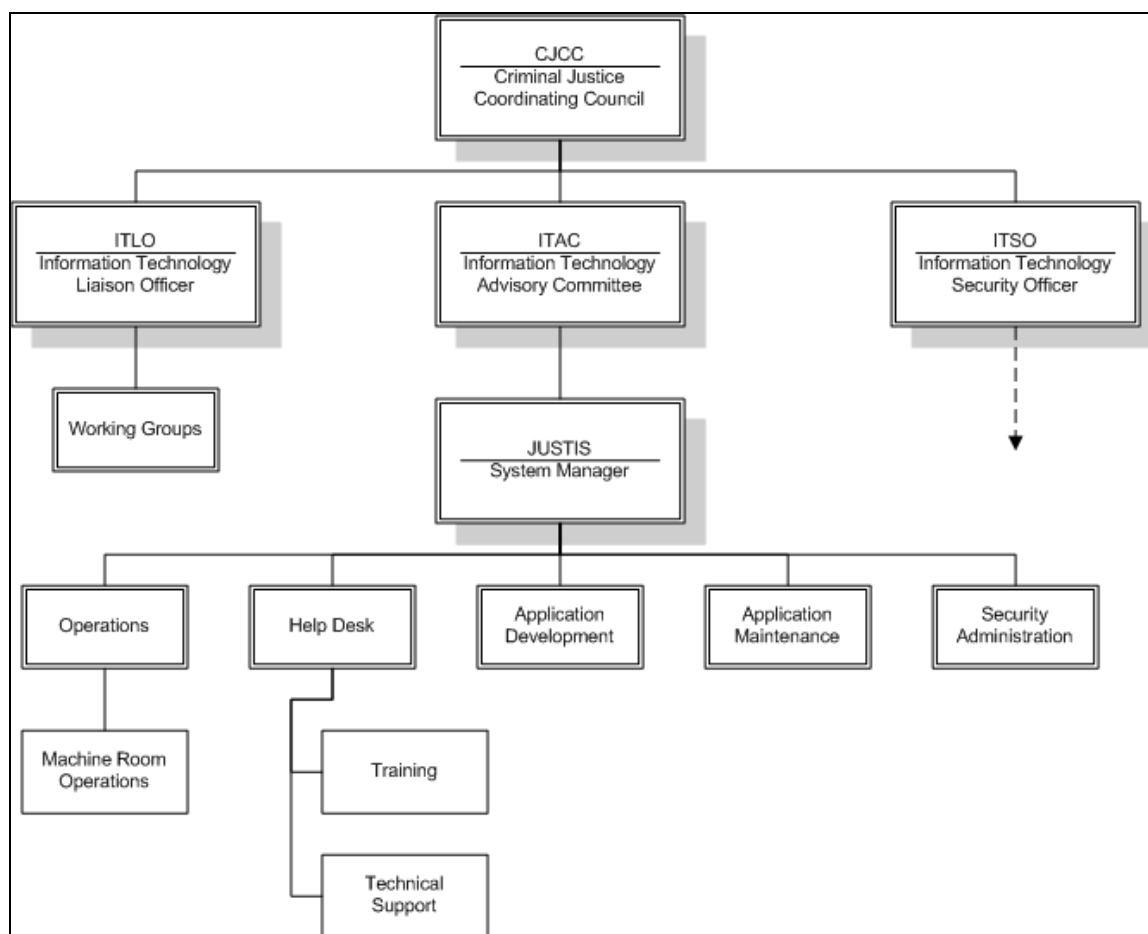


Figure 30 – Future JUSTIS Administrative and Management Structure

## 5.2.1.2 Increased Functionality

### 5.2.1.2.1 Second Chance Data Contribution - 2-A-1

The Next Step project has two segments. The first effort will use forums, round tables and interviews to establish the remaining intra-agency data requirements. The second is to work with the owner agencies to determine if they possess the data, if they will contribute the data to JUSTIS, how to modify their contribution to JUSTIS and to how manage the new data through JUSTIS.

### 5.2.1.2.2 DMV Vehicle Inquiry - 2-A-2

This is a Fast Track Project. All the groundwork for this effort was completed with the DMV Driver Inquiry. This effort will simply duplicate the current



access / query methods and codes with a different data target and new search arguments.

#### **5.2.1.2.3 Court Core Data Transfer (CCDT) - 2-A-3**

This project is the natural continuation of the initial Core Data Transfer – Arrest Data - project. With the CCDT, the offender data associated with her/his criminal case will be sent on a very frequent schedule of 15 to 30 minutes to a JUSTIS supported “push” function. This data will also be temporarily stored on FIFO transient database, with a file life of 15 days. This file will be considered as the JUSTIS CCDT “pull” functionality. This project will involve the use of a vendor lead, ITAC member chaired, Joint Application Development (JAD) program.

#### **5.2.1.2.4 Warrant Status File (WSF) - 2-A-4**

This project can be a stand alone or planned as part of the CCDT project. The WSF will be a transient file initiated by the creation of a warrant by a DC justice agency participating in JUSTIS. A vendor led, ad hoc user group or Joint Application Development (JAD) program, chaired by an ITAC member, will establish the warrant data contained in this file. The warrant will remain on the file until the warrant is no longer valid. It is expected several agencies will contribute warrant data, the bulk of which will be issued and removed by the DCSC.

#### **5.2.1.2.5 Notification System (NOT) - 2-A-5**

The JUSTIS Notification system has been defined by an ITAC member chaired Joint Application Development (JAD) program. The NOT Detailed Specification has been reviewed and accepted by the ITAC. The Specification will require a review prior to the issuance of a Statement of Work (SOW).

### **5.2.1.3 Systematic Expansion**

#### **5.2.1.3.1 Performance based System Deployment - 3-A-1**

The performance of the current JUSTIS system requires user assessment and evaluation. This will result in a minimum performance agreement /document. From that point, all future deployments, whether involving functionality, system expansion, or user expansion will be first weighed against its projected impact upon the performance agreement. If impact is projected, it will be quantified and mitigating actions will be identified. Based upon the impact projection, the ITAC will then make a Go/No Go decision. The ITAC can delegate this decision to either the ITLO or the JUSTIS System

Manager (JSM). Following deployment, the ITLO will report any financial and technical impacts upon JUSTIS and provide steps to mitigate these impacts.

## 5.2.2 *Realistically Achievable*

### 5.2.2.1 **Mission Critical - 1-B-1**

No project in this category is currently identified as Mission Critical.

### 5.2.2.2 **Increased Functionality**

#### 5.2.2.2.1 *Secure Emails - 2-B-1*

The JUSTIS system user community uses legal, confidential and restricted access documentation on a daily basis. Very often the purpose of these documents is to notify or inform another member of the justice community of immanent actions or constraints. While the document, such as a court order or a warrant, was created for rapid processing, the delivery methods currently utilized are based upon hand-to-hand delivery. The use of certificate-based, secure email and digital signatures will provide immediate delivery of these documents, guaranteeing the validity of the document, the identity of the sender and the receipt by the addressee.

#### 5.2.2.2.2 *Universal Data Dictionary - 2-B-2*

The ITAC authorized the creation of the Automated Reference Materials (ARM) system to facilitate the communication of system plans, system developments, and system data definitions. The ARM is currently accessible for inquiry only by all JUSTIS participants and for inquiry modification by selected agency personnel. As new systems are developed and implemented the ITAC indicated it would be wise to create a Universal Data Dictionary (UDD). This UDD would cross-reference the available data elements throughout the IT systems in the CJCC agencies. This cross-reference would provide views of where important data is generated and what data is associated and in what agencies the data is obtained and entered into an information system.

#### 5.2.2.2.3 *Data Quality Alliance Agency Statistics (DQAS) – 2-B-3*

The Data Quality Alliance is based upon user identification of data inconsistencies and errors, and the resulting actions by an Agency Data Quality Alliance representative. Unless the agency representative keeps an

exhaustive list of her/his findings, there will be no aggregate reporting possible. This project will track the types and occurrences of user reports and corrective actions, creating agency oriented aggregate reports upon demand.

#### *5.2.2.2.4 JUSTIS Search Engine - 2-B-4*

The JUSTIS system provides a repository of reports, research and references gathered in no other system. As the system grows it will become more and more difficult to find specific data or results. Although JUSTIS has a search engine, it is not robust enough to support rapid turn-around as the data and research grows, and the user community grows.

#### *5.2.2.2.5 Discussion Groups - 2-B-5*

The JUSTIS system can provide a central, virtual meeting room for any and all of the members of the entire DC user community. This community can discuss virtually any subject. Any individual member can initiate the discussion. Again, JUSTIS has an elementary discussion group product, but as the user community grows, the capacity of this function may quickly be outpaced.

### **5.2.2.3 Systematic Expansion**

#### *5.2.2.3.1 1997 Police Coordination Act Agencies – 3-B-1*

The ITAC has approved the invitation to the agencies of the 1997 Police Coordination Act to join JUSTIS. This expansion has been very measured to prevent any possible breach in our security program. This expansion is directly related to use of the Internet to allow access to JUSTIS. Because of the vulnerabilities of this approach, the security team has required additional methods and approaches to be designed and tested prior to initial implementation. We will work to expand this system availability as the pilot agencies' access is tested.

#### *5.2.2.3.2 U.S. District Court – 3-B-2*

The U.S. District Court (USDC) is allied with by a number of potential JUSTIS participant agencies. Several of these agencies have requested that the USDC be approached and requested to join JUSTIS as a data contributor. This would allow automated access to agencies whose mission, such a PSA, require timely access and processing of U.S. District Court offender data.

#### **5.2.2.3.3 Interstate JUSTIS Query – 3-B-3**

A number of local justice agencies that reside outside the geo-political boundaries of the District of Columbia have expressed interest in accessing JUSTIS data.

As “our” offenders are often “their” offenders, access by other agencies would be the logical extension of the JUSTIS system. This access not only builds a stronger justice community, but also answers the challenge of the U.S. Attorney General as he asks state, local and federal agencies to work more closely together.

#### **5.2.2.3.4 Interstate JUSTIS Access – 3-B-4**

A number of DC justice agencies have expressed interest in accessing systems of justice agencies that reside outside the geo-political boundaries of the District of Columbia JUSTIS. As “their” offenders are often “our” offenders, the access by our agencies would be the logical reciprocal to the extension of access by those agencies to the JUSTIS system. This access not only builds a stronger justice community, but also answers the challenge of the U.S. Attorney General as he asks state, local and federal agencies to work more closely together.

#### **5.2.2.3.5 Federal Public Defender – 3-B-5**

The inclusion of the Federal Public Defender in JUSTIS would allow limited additional data to become accessible to the FPD from a limited number of JUSTIS participants, and additional data from that agency to become available to the rest of the JUSTIS community.

### **5.2.3 Vision Oriented**

#### **5.2.3.1 Mission Critical**

##### **5.2.3.1.1 System Continuity – 1-C-1**

The deployment of JUSTIS should be expanded to serve as a stand-in process for agency processes in the event that non-JUSTIS systems are affected by a disaster or other sustained service interruption. The inherent backup and recovery nature of JUSTIS should also be exploited to provide for system-wide backup. During a major disaster - one that results in sustained downtime on user agency legacy systems - JUSTIS could also play a major role in the recovery on non-JUSTIS systems that operate on similar data. JUSTIS, then, plays a role as a provider of data redundancy that can be used

to restore non-JUSTIS systems but it also provides for functionality that will enable operations to continue during the disaster.

### 5.2.3.2 Increased Functionality

#### 5.2.3.2.1 Core Data Transfer Statistical Delivery – 2-C-1

This project would load the CDT data from both the Arrest and Court CDT processes to a predefined statistical tool. This tool would be available to both individual agencies and to the ITAC and CJCC for problem definition, alternative examination, and for program evaluation purposes.

#### 5.2.3.2.2 PD 163 – 2-C-2

The PD-163 and other justice-oriented documents would be made available to all other authorized participating JUSTIS agencies. This project is directly dependant upon the PD-163, and all other such documents, being currently maintained in a digital format, in an automated system maintained by an owner agency, and being accessible through a JUSTIS automated acquisition process.

#### 5.2.3.2.3 Soundex Inquiries – 2-C-3

Soundex inquiries greatly enhance the ability of users to locate name indexable offender records when only a portion of the name is available or when the correct spelling of the name is unknown. The use of Soundex routines is dependant the use of such algorithms in the agency legacy systems. When they are used, JUSTIS will apply the same routines and make them available to all users.

### 5.2.3.3 Systematic Expansion

#### 5.2.3.3.1 U.S. Bureau of Prisons – 3-C-1

The U.S. Bureau of Prisons, while a member of ITAC, has not become a JUSTIS user. The ITAC will again offer access to BOP and invite BOP to contribute data to the JUSTIS community.

#### 5.2.3.3.2 NCIC / NLETS – 3-C-2

While not all JUSTIS users are eligible for access to the National Crime Information System (NCIC) or the National Law Enforcement Telecommunications System (NLETS), those who do have or would have access would find it invaluable. JUSTIS can serve as either the primary or alternate conduit to these systems. JUSTIS would not store this data, but

would provide the pass-thru facility to authorized users. JUSTIS would not administer or grant access to either system, but enforce the access decisions of the MPD.

### 5.3 Proposed Phases of Implementation

Now that the gap items have been prioritized and analyzed for interdependencies, the gap items will be partitioned into phases for future release implementations of JUSTIS. Developing a phased implementation schedule is made easier when one follows along Figure 28 - JUSTIS Priority Matrix. Although the JUSTIS Priority Matrix prioritizes elements along a relative priority axis, a phased implementation requires development to be addressed in four- to six-month increments. Therefore, this section tries to follow the matrix with regard to a phased implementation and tasks do not necessarily follow the matrix. In addition to priority and interdependence, phase steps have been chosen for their simplicity of implementation relative to the value they provide. This means that early phases will combine items necessary for infrastructure support as well as items that return high value for a relatively small investment.

#### 5.3.1 Phase 4 –Second Chance Data Contribution

Following along Figure 28 - JUSTIS Priority Matrix the next logical step in JUSTIS phased implementation is the establishment of a JUSTIS Operations Staff. It is recommended at this time that the ITAC take advantage of the success of JUSTIS when considering increasing the functionality of JUSTIS by implementing the Second Chance Data Contribution - 2-A-1. The table below lists the tasks to be addressed in the next phase of JUSTIS.

Phase 4 Tasks	
Mission Critical	
	JUSTIS Staffing
Increased Functionality	
	Second Chance Data Contribution
	DMV Vehicle Data
Systematic Expansion	
	System Performance

### 5.3.2 Phase 5 –Expansion of Core Data Transfer

Given the successful implementation of the District of Columbia Superior Court new case management information system it would benefit the ITAC to take advantage and expand the current data transfer to include data from this new system. Other items to be considered this phase are Warrant Status and the development of the JUSTIS Notification System. The table below lists this phases proposed tasks.

Phase 5 Tasks	
Mission Critical	
	None
Increased Functionality	
	Core Data Transfer for Courts
	Warrant Status File
	Notification System
Systematic Expansion	
	None

### 5.3.3 Phase 6 –Increased Functionality – Secure Email

Following along Figure 28 - JUSTIS Priority Matrix the next logical step in JUSTIS phased implementation is the continued development of realistically achievable elements that increase the functionality of JUSTIS. The table below lists the tasks to be addressed in this phase of JUSTIS development.

Phase 6 Tasks	
Mission Critical	
	None
Increased Functionality	
	Secure Email
	Universal Data Dictionary
	Search Engine
Systematic Expansion	
	None



### 5.3.4 Phase 7 –Increased Functionality – Systematic Expansion

Following along Figure 28 - JUSTIS Priority Matrix the next logical step in JUSTIS phased implementation is the expansion of JUSTIS beyond the District of Columbia borders. The table below lists the tasks to be addressed in this phase of JUSTIS development.

Phase 7 Tasks	
Mission Critical	
	None
Increased Functionality	
	None
Systematic Expansion	
	1997 Police Coordination Act Agencies
	District Court
	Federal Public Defender
	Interstate Queries

### 5.3.5 Phase 8 –Vision Oriented

It is anticipated that by this time of the JUSTIS development, items categorized and discussed in section 5.2.3 Vision Oriented will have to be better defined. These items will be planned in future phases. The table below lists a recommended order for addressing these items.

Phase 8 Tasks	
Mission Critical	
	System Continuity
Increased Functionality	
	Core Data Transfer Statistical Server
	PD 163
	Soundex
Systematic Expansion	
	Bureau of Prisons
	NCIC / NLETS

## 6. Conclusion

### 6.1 JUSTIS Blueprint

JUSTIS has matured over the past three phases to a fully operational system that provides benefit to the entire District of Columbia public safety community. The next phases of JUSTIS will make this information system a critical element in the entire criminal justice process. Applications such as the JUSTIS Notification System described in section 3.4.1 of this document will integrate JUSTIS into the business process of several CJCC member agencies. Items such as the expansion of the data transfer functionality as described in section 3.4.3 will integrate JUSTIS into the IT infrastructure of the subscribing agencies.

This document illustrates the continued vision of JUSTIS. The Blueprint does this by first explaining the overall vision of JUSTIS. Future JUSTIS User Community and System describes the various functionalities that are possible when developing and implementing a solution such as JUSTIS. Identifying the vision of the system logically provides the developer and the owner of the system with an end-result against which the system can be measured at the end of any one phase.

The Blueprint goes beyond a description of just the future of JUSTIS and describes the current status of JUSTIS. Current Systems Summary provides the reader with a detailed explanation of the current status of JUSTIS and the underlying infrastructure upon which it is built.

This is followed by the Roadmap, where an analysis of sections 3 and 4 is conducted in the formulation of functional gaps. These gaps are then prioritized in this section considerate of several factors such as technical difficulty and relationship to existing and other new functionalities. The prioritized gaps are then separated into recommended phases of implementation.

This version of the Blueprint is the third iteration of the document. Throughout this document we have discussed either present functionality or future functionality of JUSTIS. Currently JUSTIS is functioning as an application of last resort in most agencies. Users access JUSTIS only when they cannot either cannot find data using their existing information systems or do not have access to data contained in another information system. With the implementation of future phases of JUSTIS, it is anticipated the JUSTIS will become a mission critical information system throughout the District of Columbia public safety community.

## 7. Glossary

**10Base-T** – One of several adaptations of the Ethernet (IEEE 802.3) standard for Local Area Networks (LANs). The 10Base-T standard (also called Twisted Pair Ethernet) uses a twisted-pair cable with maximum lengths of 100 meters.

**100Base-T** – A relatively new networking standard that supports data transfer rates up to 100 Mbps. 100BASE-T (IEEE 802.3u) is based on the older Ethernet standard. Because it is 10 times faster than Ethernet, it is often referred to as Fast Ethernet.

**Access Control List (ACL)** – A list of access control entries (ACEs), which contain information about a trustee, such as a user, group of users, or program.

**ActiveX** – A loosely defined set of technologies developed by Microsoft. An outgrowth of two other Microsoft technologies called OLE (Object Linking and Embedding) and COM (Component Object Model).

**API** – See “Application Programming Interface”.

**Applet** – A program designed to be executed from within another application. Unlike an application, applets cannot be executed directly from the operating system.

**Application Programming Interface (API)** – a set of routines, protocols, and tools for building software applications.

**Asynchronous Transfer Mode (ATM)** – A network technology based on transferring data in cells or packets of a fixed size.

**ATM** – See “Asynchronous Transfer Mode”.

**Backbone** – Network technology used to tie together multiple networks on an enterprise network.

**BearingPoint** – Formally known as KPMG Consulting, Inc.

**Blue Pages** – X.500 service that provides subject-matter listings of organizational programs and activities related to the organization such as the government blue pages.

**BOP** – Federal Bureau of Prisons

**Certificate** – See Digital Certificate.

**Certificate Authority** – A Certificate Authority (CA) issues, verifies, and revokes certificates. The Certificate Authority’s digital signature attests to the binding of the individual’s identity and his public key.

**Certificate Revocation List** – A certificate revocation list is a list of digital certificates revoked before their scheduled expiration date.

CFSA – District of Columbia Child and Family Services Agency

CGI – See “Common Gateway Interface”.

Clear Text – Information transmitted over a network in its original, unencrypted state.

Common Gateway Interface (CGI) – A specification for transferring information between a World Wide Web server and a CGI program. A CGI program is any program designed to accept and return data that conforms to the CGI specification. The program could be written in any programming language, including C, Perl, or Visual Basic.

CSOSA – Court Services and Offender Supervision Agency

DOC – District of Columbia Department of Corrections

DCSC – Superior Court for the District of Columbia

Digital Certificate – A digital certificate is a non-forgable, tamper-proof electronic document that attests to the binding of an individual's identity with his or her public key. The information contained in the certificate is verified and sealed with the digital signature of a trusted third party, known as a Certificate Authority (CA). The CA will include in the certificate a range of dates within which it is valid.

Digital Signature – A digital signature is a portion of a message encrypted with a user's private key. The recipient knows that this message and its digital signature could have come only from the owner of the private key corresponding to the public key used to decrypt. Digital signatures not only verify the identity of the signer of messages, but also ensure that the messages have not been changed since their signing.

DHCP – See “Dynamic Host Configuration Protocol.”

DMV – District of Columbia Department of Motor Vehicles

Dynamic Host Configuration Protocol (DHCP) – A protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network.

EC/EDI – Electronic Commerce (EC) – applications such as Electronic Data Interchange (EDI) for commerce between business partners (e.g., banks, suppliers, manufacturers).

Encryption/Decryption – Encryption is the scrambling of a message into an unreadable form. Decryption is the reverse: an encrypted message is made readable. A key pair controls both encryption and decryption. If either key encrypts a message or file, only the other key in that pair can decrypt it. For example, if someone encrypts a message or file with an individual's public key, only that individual's private key can decrypt it. This assures message confidentiality. A manageable way to deploy encryption in a large environment is with the use of public key cryptography.

**Ethernet** – A local-area network (LAN) protocol that uses a bus topology and supports data transfer rates of 10 Mbps.

**Extensible Markup Language (XML)** – This new standard being developed by W3C is a simplified but strict subset of SGML that has features of validation, structure, and extensibility. XML is a standardized text format designed specifically for transmitting structured data to web applications.

**FDDI** – See “Fiber Distributed Data Interface”.

**Fiber Distributed Data Interface (FDDI)** – A set of protocols for sending digital data over fiber optic cable. Generally used for WAN backbone. Supports data rates of up to 100 Mbps.

**File Transfer Protocol (FTP)** – A mechanism for transferring files between host computers over TCP/IP. FTP includes host-independent sub-commands for connecting and logging on to remote hosts; uploading and downloading files; listing directory contents; and changing the current working directory.

**Firewall** – A hardware/software device that restricts access between more than one network. A firewall is generally configured to block all externally initiated access, and to run any permitted internally initiated access via ‘proxy’ agents so that the internal computing device is never communicating directly with an external computing device.

**Frame Relay** – A packet-switching protocol for connecting devices on a Wide Area Network. Frame Relay networks support data transfer rates at T-1 (1.544 Mbps) and T-3 (45 Mbps) speeds

**FTP** – See “File Transfer Protocol”.

**Green Pages** – X.500 service that provides browsing and querying of electronic information in documents and catalogs, such as documents statistics, photographs, multimedia records, and publications.

**HTML** – See “Hypertext Markup Language”.

**HTTP** – See “Hypertext Transport Protocol”.

**Hypertext Markup Language (HTML)** – The document encoding standard used for web pages. HTML supports embedded graphics, programs, and links to other objects such as web sites, documents, points within documents, images, and files that will automatically launch other desktop applications.

**Hypertext Transport Protocol (HTTP)** – The underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

**IETF** – See “Internet Engineering Task Force”.

IMAP – See “Internet Messaging Access Protocol”.

International Organization for Standardization (ISO) – ISO is an international organization composed of national standards bodies from over 75 countries, including ANSI (American National Standards Institute).

Internet Engineering Task Force (IETF) – The main standards organization for the Internet.

IPsec – A security protocol in the network layer being developed to provide cryptographic security services that will flexibly support combinations of authentication, integrity, access control, and confidentiality.

Internet Messaging Access Protocol (IMAP) – A protocol for retrieving email messages.

Internet Service Provider (ISP) – An organization that provides a connection to the Internet.

Intranet – A network based on TCP/IP (Internet) protocols, but belonging to an organization and accessible only by the organization's members, employees, or other authorized users.

Inter-network Packet Exchange (IPX) – A networking protocol used by the Novell NetWare operating systems. IPX is a datagram protocol used for connectionless communications.

International Telecommunications Union (ITU) – An intergovernmental organization established by the United Nations to develop international standards governing telecommunications.

IPX – See “Inter-network Packet Exchange”.

ISO – See “International Organization for Standardization”.

ISP – See “Internet Service Provider”.

ITAC – Criminal Justice Coordinating Council Information Technology Advisory Committee

ITLO – Information Technology Advisory Committee Information Technology Liaison Officer.

ITU – See “International Telecommunications Union”.

Java– A high-level programming language designed to be platform-independent. Java programs can be downloaded to a client as part of an HTML document and executed on that client.

JRSA – Justice Research and Statistics Association.

kbps – Kilobits per second. Speed of data transmission in multiples of 1,024 bits (~128 characters) per second.

KPMG CONSULTING, INC. – Former name of BearingPoint, Inc.

LAN – See “Local Area Network”.

Legacy system – Generally used to refer to working applications and platforms that do not employ consensus state-of-the-art technology.

Local Area Network (LAN) – A computer network that spans a relatively small area. A LAN generally serves a single building or floor of a building.

Mailhost – A server that routes incoming as well as outgoing email. Mail software (e.g., cc:Mail, MS Exchange) packages can store messages to be accessed by users or route mail to other mailhosts.

Management Information Base (MIB) – A database of objects that can be monitored by a network management system. Both SNMP and RMON use standardized MIB formats that allows any SNMP and RMON tools to monitor any device defined by a MIB.

Mbps – Megabits per second. Speed of data transmission in multiples of 1,048,576 bits (~131,072 characters) per second.

Meta-data or Meta-information – Data about data. Meta-data describes how and when and by whom a particular set of data was collected, and how the data is formatted.

Meta tag – An HTML tag that refers to meta-information, rather than to document text.

MIB – See “Management Information Base”.

MPDC – Metropolitan Police of the District of Columbia.

Network News Transfer Protocol (NNTP) – Industry-standard method used by News group servers to receive downloads from an ISP; store the data for a predetermined amount of time, and distribute it to users upon request. The data consists of bulletin-board articles contributed by the Internet community.

NNTP – See “Network News Transfer Protocol”.

OCC – District of Columbia Office of Corporation Counsel.

OLAP – See “On-line analytical processing”.

On-line analytical processing (OLAP) – A category of software tools that provides analysis of data stored in a database. OLAP tools enable users to analyze different dimensions of multidimensional data.

PDF – See “Portable Document Format”.



PDS – Public Defender Service.

Portable Document Format (PDF) – A file format developed by Adobe Systems. Enables viewing of documents on screen as they would be printed.

Point-to-point protocol (PPP) – A protocol that allows a computer to access an Intranet or the Internet via a voice-grade telecommunications line and a modem.

POP3 – See “Post Office Protocol”.

Post Office Protocol (POP3) – A protocol used to retrieve email from a mail server.

PPP – See “Point-to-point Protocol”.

Private key – see Public key cryptography.

PSA – Pretrial Services Agency.

PSWG – ITAC Privacy and Security Working Group.

Public key – see Public key cryptography.

Public key cryptography – In a system that uses public key cryptography, each user is assigned two unique mathematically-related keys: a public key and a private key. The public key is published; the private key is kept secret, accessible only to the owner. Each key can read messages encrypted with the other key.

Push technology – Enables Internet based service delivery initiated by the information provider, rather than by the information requester.

RAS – See “Remote Access Server”.

RDBMS – See “Relational Database Management System”.

Relational Database Management System (RDBMS) – A collection of programs that enables you to store, modify, and extract information from a database.

Remote Access Server (RAS) – A computer or device that provides network access to users not directly connected to that network. Users generally access a RAS via dial-in modem or ISDN adapter.

Remote Monitoring (RMON) – A network management protocol that allows network information to be gathered at a single workstation. Whereas SNMP gathers network data from a single type of Management Information Base (MIB), RMON 1 defines nine additional MIBs that provide a much richer set of data about network usage.

RMON – See “Remote Monitoring”.

**Router** – A router is a hardware device that directs data flow between networks. The router's software determines the best path to the destination computer from the client computer.

**S/MIME** – See “Secure Multipurpose Internet Mail Extension”.

**Secure Multipurpose Internet Mail Extension (S/MIME)** – A new version of the MIME protocol that supports encryption of messages. S/MIME is based on RSA's public-key encryption technology.

**Search Engine** – Software that reads documents and builds indices to collections of documents. This allows the user to search the index for key information, as well as document text.

**Serial-line Internet protocol (SLIP)** – A protocol that allows a computer to access an Intranet or the Internet via a voice-grade telecommunications line and a modem. SLIP is gradually being replaced by PPP.

**SGML** – See “Standard Generalized Markup Language”.

**SLIP** – See “Serial-line Internet protocol”.

**SNA** – See “Systems Network Architecture”.

**SMTP** – See “Simple Mail Transport Protocol”.

**SNMP** – See “Simple Network Management Protocol”.

**Systems Network Architecture (SNA)** – A set of network protocols developed by IBM to inter-connect mainframe computers.

**Simple Network Management Protocol (SNMP)** – A set of protocols for managing complex networks. SNMP works by sending messages, called protocol data units, to different parts of a network. SNMP-compliant devices, called agents, store data about themselves in Management Information Bases (MIBs) and return this data to the SNMP requesters.

**Simple Mail Transport Protocol (SMTP)** – A protocol for sending email messages between mail servers. SMTP is also used to send messages from a mail client to a mail server.

**Standard Generalized Markup Language (SGML)** – a system for organizing and tagging elements of a document.

**T1** – A dedicated telecommunications connection supporting data rates of 1.544Mbits per second. A T-1 line actually consists of 24 individual channels, each of which supports 64Kbits per second.

T3 – A dedicated telecommunications connection supporting data rates of about 45Mbps per second. A T-3 line actually consists of 672 individual channels, each of which supports 64Kbits per second.

TCP/IP – See “Transmission Control Protocol over Internet Protocol”.

Token Ring – A network that connects computers serially, (computer-to-computer) to form a loop, rather than via a hub, such as Ethernet.

Transaction Process Monitor (TP Monitor) – TP Monitor ensures that a transaction processes to completion and ensures that proper actions are taken if it fails to complete successfully.

Transmission Control Protocol over Internet Protocol (TCP/IP) – The suite of communications protocols used to connect hosts on the Internet. TCP/IP uses several protocols, the two main ones being TCP and IP.

TWG – Criminal Justice Coordinating Council Technical Working Group

Uniform Resource Locator (URL) – The standard naming convention used to identify a presence on the world wide web. This location can be a server ([www.location.com](http://www.location.com)); a directory on a server ([www.location.com/directory](http://www.location.com/directory)); a file on a server ([www.location.com/directory/page.html](http://www.location.com/directory/page.html)); or a point on a file ([www.location.com/page.html#refpoint](http://www.location.com/page.html#refpoint)). The location is preceded by the protocol used to access the location—e.g., <http://> (for html documents) or <ftp://> (for file transfers).

URL – See “Uniform Resource Locator”.

USAO – United States Attorney’s Office

USPC – United States Parole Commission

USPO – United States Probation Office

Virtual Private Network (VPN) – A network that is constructed by using public wires to connect nodes. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

W3C – See “World Wide Web Consortium”.

WAN – See “Wide Area Network”.

Web – See “World Wide Web”. When capitalized, “Web” typically refers to the World Wide Web on the Internet; lower-case “web” usually refers to the technology, regardless of whether it is deployed on the Internet or on a private Intranet.

Web Browser – A software application used to access information on a web-based network. A browser presents HTML-formatted documents, and it generally supports other protocols such as FTP.

**Web Site** – A single Web/Internet or private web/Intranet location (generally a web server or a directory on a web server).

**White Pages** – Basic “lookup” service for X.500 directories that presents personnel specific information such as telephone numbers, office locations, physical mailing addresses, and other personal and organizational attributes.

**Wide Area Network (WAN)** – A computer network that spans a relatively large geographical area. Typically, WAN consists of two or more local-area networks (LANs).

**World Wide Web (WWW)** – A system of Internet servers that support specially formatted documents. The documents are formatted in a language called HTML that supports links to other documents, as well as graphics, audio, and video files.

**World Wide Web Consortium (W3C)** – Organization of representatives from companies around the world that develops open standards used by the world wide web, such as HTML.

**X.500** – An ISO and ITU standard that defines how global directories should be structured. X.500 directories are hierarchical with different levels for each category of information, such as country, state, and city. X.500 supports X.400 systems.

**X.509** – X.509, or ISO/IEO 9594-8, is widely recognized as the leading network and communications security architecture standard specification. Any application or device can use the standardized security and authentication services of X.509. The authentication-framework specification within X.509 addresses the handling of public keys via certificates and certificate revocation lists.

**XML** – See “Extensible Markup Language”.

**YSA** – District of Columbia Department of Human Services’ Youth Services Administration

**Yellow Pages** – X.500 service that presents detailed information on products and services to facilitate organizational procurement activities.